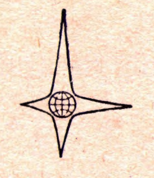


Ж.-П. Серр

Когомологии Галуа



ИЗДАТЕЛЬСТВО
„МИР“

LECTURE NOTES IN MATHEMATICS

Edited by A. Dold, Heidelberg
and B. Eckmann, Zürich

JEAN-PIERRE SERRE

Cohomologie Galoisienne

SPRINGER VERLAG
Berlin · Göttingen · Heidelberg · New York
1964

БИБЛИОТЕКА СБОРНИКА „МАТЕМАТИКА“

Ж.-П. СЕРР

КОГОМОЛОГИИ ГАЛУА

Перевод с французского
И. В. ДОЛГАЧЕВА и В. А. ИСКОВСКИХ

Под редакцией
Ю. И. МАНИНА

ИЗДАТЕЛЬСТВО „МИР“
Москва 1968

УДК 519.44

Книга написана на основе лекций, прочитанных видным французским математиком. С присущим автору мастерством в этих лекциях изложены основы теории когомологий топологических вполне несвязных групп и их многочисленные приложения к теории чисел и алгебраической геометрии, концентрирующиеся вокруг понятий когомологической размерности поля, диофантовых проблем в теории алгебраических групп и задач двойственности.

Книга представляет большой интерес для математиков различных специальностей, начиная со студентов старших курсов.

Редакция литературы по математическим наукам

Инд. 2-2-3

ПРЕДИСЛОВИЕ

Эти заметки воспроизводят с некоторыми изменениями курс лекций, прочитанный автором в Коллеж де Франс в 1962—1963 году. Кроме того, в них содержатся неопубликованные результаты Тейта (дополнение к гл. I) и Вердье, касающиеся двойственности проконечных групп.

Первоначальный вариант этих заметок, написанный Мишелем Рейно, был для меня весьма полезен. Я ему чрезвычайно благодарен.

Жан-Пьер Серр

ГЛАВА I

КОГОМОЛОГИИ ПРОКОНЕЧНЫХ ГРУПП

§ 1. ПРОКОНЕЧНЫЕ ГРУППЫ

1.1. Определение

Проконечной группой называется топологическая группа, которая является проективным пределом конечных групп (снабженных дискретной топологией). Каждая такая группа компактна и вполне несвязна. Обратно, если группа G компактна и вполне несвязна, то она обладает базой окрестностей единицы, образованной открытыми нормальными делителями U, и ее можно отождествить с $\varprojlim G/U$. Это показывает, что G проконечна.

Проконечные группы образуют категорию (морфизмами являются непрерывные гомоморфизмы), в которой существуют бесконечные произведения и проективные пределы.

Примеры. (1) Пусть L/K — расширение Галуа поля K. Группа Галуа этого расширения $G(L/K)$ является, по самому построению, проективным пределом групп Галуа $G(L_i/K)$ конечных нормальных расширений L_i/K, содержащихся в L/K; следовательно, $G(L/K)$ — проконечная группа.

(2) Компактная аналитическая группа над полем p-адических чисел $\mathbf{Q}_p$ является проконечной группой (как топологическая группа). В частности, $\mathbf{SL}_n(\mathbf{Z}_p)$, $\mathbf{Sp}_n(\mathbf{Z}_p)$, ... — проконечные группы.

(3) Пусть G — дискретная группа и $\hat{G}$ — проективный предел ее конечных факторгрупп. Группа $\hat{G}$ называется проконечной группой, ассоциированной с G. Это отделимое пополнение группы G относительно топологии, определенной подгруппами конечного индекса. В частности, ядро естественного отображения $G \to \hat{G}$ является пересечением подгрупп конечного индекса.

1.2. Подгруппы

Каждая замкнутая подгруппа H проконечной группы G является также проконечной группой. Более того, факторпространство G/H компактно и вполне несвязно.

Предложение 1. *Пусть H и K — две замкнутые подгруппы проконечной группы G и $H \supset K$. Тогда существует некоторое непрерывное сечение s: $G/H \to G/K$.*

Для доказательства этого предложения воспользуемся двумя леммами.

Лемма 1. *Пусть G — компактная группа и (S_i) — некоторое убывающее фильтрующееся семейство ее замкнутых подгрупп*[1]). *Положим $S = \bigcap S_i$. Тогда каноническое отображение*

$$G/S \to \varprojlim G/S_i$$

является гомеоморфизмом.

Действительно, это отображение инъективно и его образ всюду плотен. Так как исходное пространство компактно, то его образ также компактен, откуда следует утверждение леммы. (Можно также сослаться на Бурбаки [1], часть 3, § 7, п. 2, следствие 3, предложение 1.)

Лемма 2. *Предложение 1 справедливо в случае, когда факторпространство H/K конечно. Если, кроме того, H и K являются нормальными делителями в G, то расширение*

$$1 \to H/K \to G/K \to G/H \to 1$$

расщепляется над некоторой открытой подгруппой в G/H.

Пусть U — открытый нормальный делитель в G, такой, что $(U \cap H) \subset K$. Тогда ограничение проекции $G/K \to G/H$ на образ U инъективно (и является гомоморфизмом, если H

[1]) Убывающим фильтрующимся множеством называется такое частично упорядоченное множество E, в котором для любых двух элементов $x, y \in E$ существует элемент $z \in E$, такой, что $z \leqslant x$ и $z \leqslant y$. Двойственным образом определяется возрастающее фильтрующееся множество. — *Прим. перев.*

и K — нормальные делители; это доказывает вторую часть леммы). Обратное отображение к этому ограничению проекции есть, следовательно, некоторое сечение над образом U в G/H (который открыт), с помощью сдвигов его можно продолжить до сечения над G/H.

Теперь можно доказать предложение 1. Пусть X — множество пар (S, s), где S — замкнутая подгруппа в G, такая, что $K \subset S \subset H$, и s — некоторое непрерывное сечение s: $G/H \to G/S$. Множество X упорядочено очевидным способом. Кроме того, оно является индуктивным (лемма 1) и из леммы 2 легко выводится, что при $S = K$ элемент (S, s) является максимальным в X. Предложение 1 следует теперь из леммы Цорна.

1.3. Индексы

Назовем сверхнатуральным числом формальное произведение $\prod p^{n_p}$, где p пробегает множество всех простых чисел и n_p — целое неотрицательное число или $+\infty$. Очевидным образом определяются произведение, НОД и НОК любого семейства сверхнатуральных чисел.

Пусть G — проконечная группа и H — замкнутая подгруппа в G. *Индекс* $(G:H)$ подгруппы H в G определяется как НОК индексов $(G/U : H/(H \cap U))$, где U пробегает множество открытых нормальных делителей в G. Легко видеть, что это также НОК индексов $(G:V)$ всех открытых подгрупп V, содержащих H.

Предложение 2. (i) *Если $K \subset H \subset G$ — проконечные группы, то имеет место равенство*

$$(G:K) = (G:H)(H:K);$$

(ii) *если (H_i) — убывающее фильтрующееся семейство замкнутых подгрупп в G и если $H = \bigcap H_i$, то*

$$(G:H) = \text{НОК}\,(G:H_i);$$

(iii) *для того чтобы подгруппа H была открыта в G, необходимо и достаточно, чтобы индекс $(G:H)$ был натуральным числом (т. е. элементом из* $\mathbf{N}$).

Доказательство (i). Пусть U — открытый нормальный делитель в G. Положим $G_U = G/U$, $H_U = H/(H \cap U)$,

$K_U = K/(K \cap U)$. Имеем включения $G_U \supset H_U \supset K_U$, откуда $(G_U : K_U) = (G_U : H_U)(H_U : K_U)$. Согласно определению, НОК $(G_U : K_U) = (G : K)$ и НОК $(G_U : H_U) = (G : H)$. С другой стороны, подмножество нормальных делителей вида $H \cap U$ является конфинальным [1]) в множестве всех открытых нормальных делителей в H, следовательно, НОК $(H_U : K_U) = (H : K)$, что доказывает (i).

Утверждения (ii) и (iii) получаются немедленно.

Отметим, что можно говорить, в частности, о *порядке* $(G : 1)$ проконечной группы G.

1.4. Про-p-группы и силовские p-группы

Пусть p — простое число. Проконечная группа H называется *про-p-группой*, если она является проективным пределом p-групп, или, что то же самое, если ее порядок есть некоторая степень p (конечная или бесконечная, разумеется). Пусть G — проконечная группа. Подгруппа H в G называется *силовской* p-подгруппой, если она про-p-группа и индекс $(G : H)$ взаимно прост с p.

Предложение 3. *Каждая проконечная группа G содержит силовские p-подгруппы, и все они сопряжены.*

Воспользуемся следующей леммой (Бурбаки [1], гл. 1, приложение, теорема 1):

Лемма 3. *Проективный предел непустых конечных множеств непуст.*

Пусть X — семейство открытых нормальных делителей в G. Для каждого $U \in X$ обозначим через $P(U)$ множество силовских p-подгрупп конечной группы G/U. Применяя лемму 3 к проективной системе $P(U)$, получаем по крайней мере одно согласованное семейство H_U силовских p-подгрупп групп G/U. Легко проверить, что $H = \varprojlim H_U$ является силовской p-подгруппой в G; это доказывает первую часть предложения. Аналогично доказывается и вторая часть утверждения. Для любых двух силовских p-подгрупп H и H' группы G обозначим через $Q(U)$

---

[1]) Подмножество A частично упорядоченного множества E называется конфинальным, если для всякого элемента $x \in E$ существует элемент $y \in A$, такой, что $x \leqslant y$. — *Прим. перев.*

множество элементов $x \in G/U$, которые переводят образ H в образ H' в G/U. Применяя лемму 3 к $Q(U)$, видим, что $\varprojlim Q(U) \neq \emptyset$, следовательно, существует $x \in G$, такой, что $xHx^{-1} = H'$.

Аналогичными рассуждениями доказывается:

Предложение 4. (а) *Всякая про-p-группа, содержащаяся в G, содержится в некоторой силовской p-подгруппе группы G.*

(б) *Пусть $G \to G'$ — сюръективный морфизм, тогда образ силовской p-подгруппы группы G является силовской p-подгруппой группы G'.*

Примеры. (1) Группа $\hat{\mathbf{Z}}$ содержит в качестве силовской p-подгруппы группу целых p-адических чисел $\mathbf{Z}_p$.

(2) Если G — компактная аналитическая группа над $\mathbf{Q}_p$, то ее силовские p-подгруппы *открыты* в ней (этот результат следует из хорошо известного описания локальной структуры этих групп). Порядок группы G есть, следовательно, произведение целого натурального числа на некоторую степень p.

(3) Пусть G — дискретная группа. Проективный предел ее факторгрупп, являющихся p-группами, есть про-p-группа, которая обозначается через $\hat{G}_p$ и называется *p-пополнением* группы G. Это также наибольшая факторгруппа группы $\hat{G}$, являющаяся про-p-группой.

Упражнение. Пусть k — узел в $\mathbf{R}^3$ [1]) и $G = \pi_1(\mathbf{R}^3 - k)$ — „группа узла k“. Показать, что p-пополнение группы G изоморфно $\mathbf{Z}_p$.

1.5. Свободные про-p-группы

Пусть I — некоторое множество и $L(I)$ — *свободная* дискретная группа, порожденная элементами x_i, перенумерованными индексами из I. Пусть X — семейство нормальных делителей M из $L(I)$, таких, что:

а) $L(I)/M$ — конечная p-группа,

б) M содержит почти все x_i (т. е. все, кроме конечного числа).

---

[1]) Узел — это гомеоморфный образ окружности, см. Кроуэлл и Фокс [1*]. — *Прим. перев.*

Положим $F(I) = \varprojlim L(I)/M$. Группа $F(I)$ является про-p-группой и называется *свободной про-p-группой*, порожденной элементами x_i. Название „свободная" оправдывается следующим результатом:

Предложение 5. *Пусть G — про-p-группа. Тогда морфизмы группы $F(I)$ в G находятся в биективном соответствии с семействами $(g_i)_{i \in I}$ элементов из G, которые стремятся к нулю относительно фильтра, образованного дополнениями конечных подмножеств.*

Более точно, каждому морфизму $f\colon F(I) \to G$ сопоставляется семейство $(g_i) = (f(x_i))$. Очевидно, что получаемое таким образом соответствие является биективным.

Замечание. Наряду с $F(I)$ можно определить группу $F_s(I)$ как проективный предел групп $L(I)/M$, где нормальный делитель M удовлетворяет только условию а). Она является p-пополнением $L(I)$; морфизмы $F_s(I)$ в про-p-группу G находятся в биективном соответствии со *всевозможными* семействами $(g_i)_{i \in I}$ элементов из G. Мы увидим дальше, что группа $F_s(I)$ также *свободна*, т. е. изоморфна группе $F(J)$ для подходящего множества J.

В случае когда $I = [1, n]$, мы пишем $F(n)$ вместо $F(I)$. Группа $F(n)$ называется *свободной про-p-группой ранга n*. Имеет место соотношение $F(0) = \{1\}$, и $F(1)$ изоморфна аддитивной группе $\mathbf{Z}_p$. Дадим некоторое явное описание группы $F(n)$.

Пусть $A(n)$ — алгебра ассоциативных формальных рядов (не обязательно коммутативных) от n неизвестных $t_1, \ldots, t_n$ с коэффициентами из $\mathbf{Z}_p$ (это то, что Лазар называет „алгеброй Магнуса"). [Читатель, которому не нравятся „не обязательно коммутативные формальные ряды", может определить $A(n)$ как пополнение тензорной алгебры $\mathbf{Z}_p$-модуля $(\mathbf{Z}_p)^n$.] Снабженная топологией покоэффициентной сходимости, $A(n)$ превращается в компактное топологическое кольцо. Пусть U — мультипликативная группа элементов из $A(n)$, свободные члены которых равны 1. Легко проверить, что U — про-p-группа. Поскольку она содержит семейство элементов вида $1 + t_i$, предложение 5 показывает, что существует морфизм $\theta\colon F(n) \to U$, отображающий каждый элемент x_i в $1 + t_i$.

Предложение 6 (Лазар). *Морфизм* $\theta\colon F(n) \to U$ *инъективен.*

[Группу $F(n)$ можно отождествить, следовательно, с замкнутой подгруппой группы U, порожденной элементами $1+t_i$.]

Докажем даже более сильный результат. Прежде чем его сформулировать, условимся называть *групповой алгеброй* про-p-группы G проективный предел групповых алгебр над $\mathbf{Z}_p$ конечных факторгрупп группы G. Определенную таким образом алгебру будем обозначать через $\mathbf{Z}_p[[G]]$. Имеет место

Предложение 7. *Существует непрерывный изоморфизм* α *алгебры* $\mathbf{Z}_p[[F(n)]]$ *на* $A(n)$, *который переводит* x_i *в* $1+t_i$.

Без труда определяется гомоморфизм $\alpha\colon \mathbf{Z}_p[[F(n)]] \to$ $\to A(n)$. С другой стороны, пусть I — пополняющий идеал в $\mathbf{Z}_p[[F(n)]]$[1]; тогда из элементарных свойств конечных p-групп следует, что существует непрерывный гомоморфизм

$$\beta\colon A(n) \to \mathbf{Z}_p[[F(n)]],$$

отображающий t_i в $x_i - 1$. Осталось только проверить, что $\alpha \circ \beta = 1$ и $\beta \circ \alpha = 1$, а это очевидно. Доказательство закончено.

Замечания. 1. В случае когда $n=1$, предложение 7 показывает, что групповая алгебра группы $\Gamma = \mathbf{Z}_p$ изоморфна алгебре $\mathbf{Z}_p[[T]]$, которая является превосходным регулярным локальным кольцом размерности 2. Из этого исходил Ивасава, изучая „Г-модули".

2. В диссертации Лазара [L] группа $F(n)$ изучена подробно с помощью предложений 6 и 7. Например, если рассмотреть на $A(n)$ фильтр степеней пополняющего идеала I. то индуцируемая им фильтрация на $F(n)$ совпадает с фильтрацией, определяемой центральным рядом в $F(n)$, а ассоциированная с ней градуированная алгебра

---

[1]) Пополняющий идеал — ядро пополняющего гомоморфизма, см. Картан, Эйленберг [1], гл. VIII. — *Прим. перев.*

является свободной $\mathbf{Z}_p$-алгеброй Ли, порожденной классами T_i элементов t_i. Интересна также и фильтрация, определенная степенями идеала (p, I).

§ 2. КОГОМОЛОГИИ

2.1. Дискретные G-модули

Пусть G — проконечная группа. Дискретные абелевы группы, на которых непрерывно действует группа G, образуют абелеву категорию $\mathscr{C}_G$, являющуюся полной подкатегорией[1]) категории всех G-модулей. Утверждение „G-модуль A принадлежит $\mathscr{C}_G$“ означает, что стабилизатор каждого элемента из A открыт в G или что $A = \bigcup A^U$, где U пробегает множество всех открытых подгрупп в G (A^U означает, как обычно, подгруппу элементов из A, инвариантных относительно U).

Всякий объект A из $\mathscr{C}_G$ будем называть дискретным G-модулем (или просто G-модулем, если это не будет приводить к недоразумению). С помощью таких модулей определим когомологии группы G.

2.2. Коцепи, коциклы, когомологии

Пусть $A \in \mathscr{C}_G$. Обозначим через $C^n(G, A)$ множество непрерывных отображений G^n в A (заметим, что поскольку модуль A дискретен, то „непрерывность“ эквивалентна „локальной постоянности“). Определим кограничный оператор

$$d\colon C^n(G, A) \to C^{n+1}(G, A)$$

с помощью обычной формулы

$$(df)(g_1, \ldots, g_{n+1}) = g_1 f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n).$$

---

[1]) Подкатегория $\mathscr{C}'$ категории $\mathscr{C}$ называется полной подкатегорией, если для любых двух объектов из $\mathscr{C}'$ $\mathrm{Hom}_{\mathscr{C}}(X, Y) = \mathrm{Hom}_{\mathscr{C}'}(X, Y)$. — *Прим. перев.*

Так получается комплекс $C^*(G, A)$, группы когомологий которого $H^q(G, A)$ называются *группами когомологий группы G с коэффициентами в A.*

В случае когда G — конечная группа, получается обычное определение когомологий конечных групп. Общий случай сводится к этому благодаря следующему предложению:

Предложение 8. *Пусть (G_i) — проективная система проконечных групп и (A_i) — индуктивная система дискретных G_i-модулей (гомоморфизмы $A_i \to A_j$ должны быть согласованы в очевидном смысле с морфизмами $G_j \to G_i$). Положим $G = \varprojlim G_i$ и $A = \varinjlim A_i$. Тогда для каждого $q \geqslant 0$ имеет место соотношение*

$$H^q(G, A) = \varinjlim H^q(G_i, A_i).$$

Действительно, легко видеть, что канонический гомоморфизм

$$\varinjlim C^*(G_i, A_i) \to C^*(G, A)$$

является изоморфизмом, откуда, переходя к когомологиям, получаем требуемый результат.

Следствие 1. *Пусть A — дискретный G-модуль. Тогда для каждого $q \geqslant 0$ имеем*

$$H^q(G, A) = \varinjlim H^q(G/U, A^U),$$

где U пробегает множество всех открытых нормальных делителей в G.

Действительно, $G = \varprojlim G/U$ и $A = \varinjlim A^U$.

Следствие 2. *Пусть A — дискретный G-модуль. Тогда для каждого $q \geqslant 0$ имеем*

$$H^q(G, A) = \varinjlim H^q(G, B),$$

где B пробегает множество G-подмодулей конечного типа в A.

Действительно, $A = \lim B$.

Следствие 3. *Для* $q \geqslant 1$ *группы* $H^q(G, A)$ *периодичны.*

В случае когда G конечна, это классический результат. Общий случай выводится из этого благодаря следствию 1.

Поэтому все можно легко свести к случаю конечных групп, который хорошо известен (см., например, книгу Картана, Эйленберга „Гомологическая алгебра", цитируемую в дальнейшем как [M], или книгу автора „Corps Locaux", цитируемую как [CL] [1]). Таким способом выводится, например, что $H^q(G, A)$ равны нулю при $q \geqslant 1$, если A — инъективный модуль в $\mathscr{C}_G$ (A^U тогда инъективны над G/U). Так как категория $\mathscr{C}_G$ обладает достаточным количеством инъективных (но не проективных!) объектов, мы убеждаемся, что функторы $H^q(G, \;)$ являются *производными функторами* функтора A^G, как и должно быть.

2.3. Малые размерности

$H^0(G, A) = A^G$, как обычно.

$H^1(G, A)$ есть группа классов *непрерывных* скрещенных гомоморфизмов G в A.

$H^2(G, A)$ есть группа классов непрерывных *систем факторов* G в A. Если модуль A *конечен*, то это также группа классов расширений группы G с помощью группы A (доказательство стандартное и основывается на существовании непрерывного сечения, установленном в п. 1.2).

Замечание. Этот последний пример подсказывает, как можно, исходя из непрерывных коцепей, определить $H^q(G, A)$ в случае, когда A — *произвольный* топологический G-модуль. Такого рода когомологии действительно встречаются в приложениях. С одним из таких примеров мы познакомимся позднее.

2.4. Функториальность

Пусть G и G' — две проконечные группы и $f\colon G \to G'$ — некоторый морфизм. Пусть $A \in \mathscr{C}_G$ и $A' \in \mathscr{C}_{G'}$. Можно говорить тогда о морфизме $h\colon A' \to A$, *совместимом* с f

---

[1]) На русском языке подробное изложение теории когомологий конечных групп имеется в книге Картана, Эйленберга [M], гл. XII, а также в книге Маклейна [1]. — *Прим. перев.*

(это некоторый G-морфизм, причем структура G-модуля[1]) на A' определена с помощью морфизма f). Каждая пара совместимых морфизмов (f, h) определяет гомоморфизм групп когомологий

$$H^q(G', A') \to H^q(G, A), \qquad q \geqslant 0.$$

В частности, когда $G' = H$ — замкнутая подгруппа в G и $A = A'$ — дискретный G-модуль, получаем гомоморфизм *ограничения*

$$\mathrm{Res}\colon H^q(G, A) \to H^q(H, A), \qquad q \geqslant 0.$$

---

[1]) Пусть G и G' — две группы и $f\colon G' \to G$ — некоторый гомоморфизм. На всяком G-модуле A можно определить структуру G'-модуля, полагая

$$s' \cdot a = f(s') \cdot a, \qquad s' \in G', \quad a \in A.$$

Определенный таким образом G'-модуль обычно обозначается через f^*A и называется обратным образом модуля A относительно гомоморфизма f. Очевидно, что A^G является подгруппой группы $(f^*A)^{G'}$. Это определяет морфизм функторов $H^0(G, A)$ в $H^0(G', f^*A)$, и так как $H^q(G', f^*A)$, $q \geqslant 0$, составляют когомологический функтор (относительно A), то из свойства универсальности производных функторов (см., например, Гротендик [1], п. 2.2, 2.3) следует, что этот морфизм продолжается до морфизма когомологического функтора $\{H^q(G, \,), \delta\}$ в когомологический функтор $\{H^q(G', f^*), \delta\}$. В частности, для всякого целого числа $q \geqslant 0$ и всякого G-модуля A имеет место гомоморфизм

$$f_q^*\colon \ H^q(G, A) \to H^q(G', f^*A).$$

Более общо, рассмотрим G'-модуль A' и некоторый гомоморфизм $g\colon A \to A'$. Будем говорить, что гомоморфизмы f и g совместимы, если $g(f(s')a) = s' \cdot g(a)$ для всех $s' \in G'$ и $a \in A$. Это равносильно утверждению, что гомоморфизм g является G'-морфизмом модуля f^*A в модуль A'. В таком случае g определяет гомоморфизм

$$g_q^*\colon \ H^q(G', f^*A) \to H^q(G', A')$$

и композиция $g_q^* \circ f_q^*$ задает гомоморфизм

$$(f, g)_q^*\colon \ H^q(G, A) \to H^q(G', A'),$$

ассоциированный с парой совместимых гомоморфизмов (f, g) (см. [CL], гл. VII, § 5). — *Прим. перев.*

2 Зак. 1202

Если H имеет *конечный индекс* n в G, то можно определить (например, с помощью перехода к пределу, отправляясь от конечных групп) гомоморфизм *коограничения*

$$\mathrm{Cor}: H^q(H, A) \to H^q(G, A).$$

Имеем $\mathrm{Cor} \circ \mathrm{Res} = n$, откуда следует

Предложение 9. *Если $(G:H) = n$, то ядро гомоморфизма* $\mathrm{Res}: H^q(G, A) \to H^q(H, A)$ *аннулируется умножением на n.*

Следствие. *Если индекс $(G:H)$ взаимно прост с простым числом p, то* Res *инъективен на p-примарной компоненте группы $H^q(G, A)$.*

[Это следствие особенно полезно в случае, когда H — силовская p-подгруппа группы G.]

В случае когда индекс $(G:H)$ конечен, следствие непосредственно вытекает из предыдущего предложения. Общий случай можно свести к этому, если представить H в виде пересечения открытых подгрупп и применить предложение 8.

2.5. Индуцированные модули

Пусть H — замкнутая подгруппа проконечной группы G и $A \in \mathscr{C}_H$. Индуцированный модуль $A^* = M_G^H(A)$ определяется как множество непрерывных отображений $a^*: G \to A$, таких, что $a^*(hx) = ha^*(x)$, где $h \in H$, $x \in G$. Группа G действует на A^* по формуле

$$(ga^*)(x) = a^*(xg).$$

В случае, когда $H = \{1\}$, мы пишем просто $M_G(A)$; получаемые таким способом G-модули называются *индуцированными* (коиндуцированными в терминологии [CL]).

Если каждому элементу $a^* \in M_G^H(A)$ сопоставить его значение в 1, получится гомоморфизм $M_G^H(A) \to A$, который совместим с естественным вложением H в G (см. п. 2.4). Он определяет гомоморфизмы

$$H^q(G, M_G^H(A)) \to H^q(H, A).$$

Предложение 10. *Гомоморфизмы* $H^q(G, M_G^H(A)) \to H^q(H, A)$, *определенные выше, являются изоморфизмами.*

Заметим прежде всего, что для любого $B \in \mathscr{C}_G$ имеет место изоморфизм $\mathrm{Hom}_G(B, M_G^H(A)) = \mathrm{Hom}_H(B, A)$. Это показывает, что функтор M_G^H переводит инъективные объекты в инъективные. Так как, с другой стороны, он точен, то предложение следует из стандартной теоремы сравнения [1]).

Следствие. *Когомологии индуцированного модуля равны нулю в размерностях* $q \geqslant 1$.

Это частный случай предыдущего предложения, когда $H = \{1\}$.

Предложение 10 (иногда называемое „теоремой Шапиро") очень часто используется: оно позволяет заменять когомологии подгруппы когомологиями самой группы. Укажем, как с этой точки зрения можно рассматривать гомоморфизмы Res и Cor.

(а) Пусть $A \in \mathscr{C}_G$. Определим инъективный гомоморфизм

$$i\colon\ A \to M_G^H(A),$$

полагая

$$i(a)(x) = xa.$$

При переходе к когомологиям немедленно проверяется, что мы получаем гомоморфизм *ограничения*

$$\mathrm{Res}\colon\ H^q(G, A) \to H^q(G, M_G^H(A)) = H^q(H, A).$$

[Случай $H = \{1\}$ доставляет некоторый *стирающий функтор* [2]), используемый в дальнейшем.]

[1]) Имеется в виду следующий факт: два универсальных когомологических функтора, совпадающие в нулевой размерности, совпадают всюду (см. Гротендик [1], гл. II, п. 2.2, 2.3). — *Прим. перев.*

[2]) Аддитивный функтор F из категории $\mathscr{C}$ в категорию $\mathscr{C}'$ называется *стирающим*, если для всякого $A \in \mathscr{C}$ можно найти мономорфизм $u\colon A \to M$, такой, что $F(u) = 0$. Если в категории $\mathscr{C}$ каждый объект A допускает мономорфизм в инъективный объект M, то свойство функтора F быть стирающим эквивалентно обращению его в нуль на инъективных объектах. — *Прим. перев.*

(б) Предположим, что H имеет конечный индекс в G, и пусть $A \in \mathscr{C}_G$. Определим сюръективный G-гомоморфизм

$$\pi\colon\ M_G^H(A) \to A,$$

полагая

$$\pi(a^*) = \sum_{x \in G/H} x a^*(x^{-1});$$

эта формула имеет смысл, так как элемент $xa^*(x^{-1})$ зависит только от класса x по модулю H. При переходе к когомологиям π дает гомоморфизм *коограничения*

$$\mathrm{Cor}\colon\ H^q(H,\ A) = H^q\big(G,\ M_G^H(A)\big) \to H^q(G,\ A).$$

В самом деле, это морфизм когомологических функторов, который в размерности нуль совпадает с гомоморфизмом взятия нормы.

Упражнение. Предположим, что H является *нормальным делителем* в G. Если $A \in \mathscr{C}_G$, то можно определить действие G на $M_G^H(A)$, полагая

$${}^g a^*(x) = g a^*(g^{-1}x).$$

Показать, что H в этом случае действует тривиально, что позволяет рассматривать действие G/H на $M_G^H(A)$. Показать, что так определенное действие *коммутирует* с действием G, определенным в тексте. Получить отсюда некоторое действие G/H на группы $H^q\big(G,\ M_G^H(A)\big) = H^q(H,\ A)$. Показать, что оно совпадает с естественным действием (см. следующий пункт).

Показать, что $M_G^H(A)$ изоморфен $M_{G/H}(A)$. В случае когда индекс $(G : H)$ конечен, вывести формулы

$$H^0\big(G/H,\ M_G^H(A)\big) = A \quad \text{и} \quad H^i\big(G/H,\ M_G^H(A)\big) = 0 \ \text{ для } i \geqslant 1.$$

2.6. Дополнения

Оставляем читателю самостоятельно проработать следующие пункты (которые будут использоваться в дальнейшем):

(а) $\cup$-*произведения.*

Различные свойства, особенно поведение в точных последовательностях. Формулы

$$\operatorname{Res}(x \cdot y) = \operatorname{Res}(x) \cdot \operatorname{Res}(y),$$
$$\operatorname{Cor}(x \cdot \operatorname{Res}(y)) = \operatorname{Cor}(x) \cdot y.$$

(б) *Спектральная последовательность расширений групп* [1]).

Если H — замкнутый нормальный делитель в G и $A \in \mathscr{C}_G$, то группа G/H естественно действует на $H^q(H, A)$ и это действие непрерывно. Имеет место спектральная последовательность

$$H^p(G/H, H^q(H, A)) \Rightarrow H^n(G, A).$$

В малых размерностях она порождает следующую точную последовательность:

$$0 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A)^{G/H} \to$$
$$\to H^2(G/H, A^H) \to H^2(G, A).$$

Упражнения (соотношения между когомологиями дискретных и проконечных групп).

1) Пусть G — дискретная группа, и пусть $G \to K$ — некоторый гомоморфизм G в проконечную группу K. Предположим, что образ G всюду плотен в K. Тогда для каждого модуля $M \in \mathscr{C}_K$ имеют место гомоморфизмы

$$H^q(K, M) \to H^q(G, M), \qquad q \geqslant 0.$$

Мы ограничимся подкатегорией $\mathscr{C}'_K$ категории $\mathscr{C}_K$, образованной конечными K-модулями M.

(а) Показать эквивалентность следующих четырех свойств:

A_n. *Гомоморфизм $H^q(K, M) \to H^q(G, M)$ биективен при $q \leqslant n$ и инъективен при $q = n+1$ (для всех $M \in \mathscr{C}'_K$).*

B_n. *Гомоморфизм $H^q(K, M) \to H^q(G, M)$ сюръективен при $q \leqslant n$.*

---

[1]) Спектральная последовательность расширений групп в литературе обычно называется спектральной последовательностью Хохшильда — Серра. — *Прим. перев.*

C_n. *Для каждого* $x \in H^q(G, M)$, $1 \leqslant q \leqslant n$, *существует модуль* $M' \in \mathscr{C}_K$, *содержащий* M, *такой, что* x *индуцирует* 0 *в* $H^q(G, M')$.

D_n. *Для каждого* $x \in H^q(G, M)$, $1 \leqslant q \leqslant n$, *существует подгруппа* G_0 *в* G, *являющаяся прообразом некоторой открытой подгруппы в* K, *такая, что* x *индуцирует* 0 *в* $H^q(G_0, M)$.

[Импликации $A_n \Rightarrow B_n \Rightarrow C_n$ очевидны, как и $B_n \Rightarrow D_n$. Импликация $C_n \Rightarrow A_n$ доказывается индукцией по n. Наконец, $D_n \Rightarrow C_n$ можно доказать, взяв за M' индуцированный модуль $M_G^{G_0}(M)$.]

(б) Показать, что свойства $A_0, \ldots, D_0$ выполнены всегда. Показать, что свойства $A_1, \ldots, D_1$ выполнены в случае, когда K — проконечная группа $\hat{G}$, ассоциированная с G.

(в) Возьмем за G дискретную группу $\mathbf{PGL}(2, \mathbf{C})$. Показать, что $\hat{G} = \{1\}$ и что $H^2(G, \mathbf{Z}/2\mathbf{Z}) \neq 0$ (использовать расширение G, порожденное $\mathbf{SL}(2, \mathbf{C})$). Вывести отсюда, что группа G не обладает свойством A_2.

(г) Пусть K_0 — открытая подгруппа в K и G_0 — ее полный прообраз в G. Показать, что если гомоморфизм $G \to K$ обладает свойством A_n, то то же самое справедливо и для гомоморфизма $G_0 \to K_0$, и обратно.

2) [Здесь и далее мы говорим, что G удовлетворяет условию A_n, если это условие выполнено для канонического отображения $G \to \hat{G}$. Группу G будем называть „хорошей", если она удовлетворяет условиям A_n при всех n.]

Пусть $E/N = G$ — некоторое расширение группы G, удовлетворяющей условию A_2.

(а) Предположим сначала, что группа N *конечна*. Пусть I — коммутант подгруппы N в E. Показать, что I имеет конечный индекс в E. Вывести отсюда, что группа $I/(I \cap N)$ удовлетворяет условию A_2 (применить 1, г), потому что существует подгруппа E_0 конечного индекса в E, такая, что

$$E_0 \cap N = \{1\}.$$

(б) Предположим теперь, что N имеет *конечный тип*. Показать (используя (а)), что всякая подгруппа конечного

индекса в N содержит подгруппу вида $E_0 \cap N$, где E_0 — подгруппа конечного индекса в E. Вывести отсюда точную последовательность

$$1 \to \hat{N} \to \hat{E} \to \hat{G} \to 1.$$

(в) Предположим, кроме того, что N и G — „хорошие“ группы и что группы $H^q(N, M)$ конечны для любого конечного E-модуля M. Показать, что E также „хорошая“ (сравнить спектральные последовательности для расширений $\hat{E}/\hat{N} = \hat{G}$ и $E/N = G$).

(г) Показать, что последовательные расширения свободных групп конечного типа являются „хорошими“ группами. Этот результат имеет приложения к группам кос[1]).

(д) Показать, что $\mathbf{SL}(2, \mathbf{Z})$ — „хорошая“ группа (можно использовать то, что она содержит свободную подгруппу конечного индекса).

§ 3. КОГОМОЛОГИЧЕСКАЯ РАЗМЕРНОСТЬ

3.1. Когомологическая p-размерность

Пусть p — простое число и G — некоторая проконечная группа. *Когомологической p-размерностью* группы G (обозначается через $\mathrm{cd}_p(G)$) называется нижняя грань целых чисел n, удовлетворяющих следующему условию:

(*) Для всякого дискретного периодического G-модуля A и для всякого целого числа $q > n$ p-примарная компонента группы $H^q(G, A)$ равна нулю.

(Разумеется, если такого целого n не существует, то $\mathrm{cd}_p(G) = +\infty$.)

Положим $\mathrm{cd}(G) = \sup \mathrm{cd}_p(G)$. Тогда $\mathrm{cd}(G)$ называется *когомологической размерностью* группы G.

Предложение 11. *Пусть G — проконечная группа, p — простое число и n — некоторое целое число. Тогда эквивалентны следующие условия*:

(i) $\mathrm{cd}_p(G) \leqslant n$;

---

[1]) О группах кос см., например, Артин [1*]. — *Прим. перев.*

(ii) $H^q(G, A) = 0$ *для каждого* $q > n$ *и для всякого дискретного* G*-модуля* A, *являющегося* p*-примарной периодической группой*;

(iii) $H^{n+1}(G, A) = 0$, *если* A — *простой дискретный* G*-модуль, аннулируемый умножением на* p.

Пусть A — периодический G-модуль и $A = \sum A(p)$ — его разложение на p-примарные компоненты. Легко видеть, что группа $H^q(G, A(p))$ отождествляется с p-примарной компонентой группы $H^q(G, A)$. Отсюда следует эквивалентность условий (i) и (ii). Импликация (ii)$\Rightarrow$(iii) тривиальна. С другой стороны, если выполнено условие (iii), то рассуждения типа „отвинчивания" (dévissage)[1]) показывают, что $H^{n+1}(G, A) = 0$, когда модуль A конечен и аннулируется некоторой степенью p. Переходом к индуктивному пределу (см. предложение 8, следствие 2) этот же результат распространяется на произвольные дискретные G-модули A, являющиеся p-периодическими группами. Отсюда с помощью индукции по q выводим справедливость условия (ii): именно вкладываем A в индуцированный модуль $M_G(A)$ и применяем предположение индукции к G-модулю $M_G(A)/A$, который также является p-периодическим.

Предложение 12. *Предположим, что* $\mathrm{cd}_p(G) \leqslant n$, *и пусть* G*-модуль* A *дискретен и* p*-делим* (т. е. гомоморфизм p: $A \to A$ сюръективен). *Тогда* p*-примарная компонента группы* $H^q(G, A)$ *равна нулю при* $q > n$.

Точная последовательность G-модулей

$$0 \to A_p \to A \xrightarrow{p} A \to 0$$

---

[1]) Суть метода „отвинчивания" заключается в следующем. Предположим, что модуль A включен в точную последовательность

$$0 \to A_1 \to A \to A_2 \to 0$$

и когомологическое утверждение, которое мы хотим доказать для A, известно для A_2. Тогда соответствующая точная последовательность когомологий позволяет свести это утверждение к аналогичному утверждению для модуля A_1, который в некотором смысле более прост, чем A, например, если A конечен, то A_1 имеет меньший порядок. Последовательно отщепляя от A фактормодули типа A_2, мы можем получить таким образом доказательство утверждения. — *Прим. перев.*

порождает точную последовательность групп когомологий

$$H^q(G, A_p) \to H^q(G, A) \xrightarrow{p} H^q(G, A).$$

При $q > n$ по предположению $H^q(G, A_p) = 0$. Гомоморфизм умножения на p в группе $H^q(G, A)$ является, следовательно, инъективным. Это, очевидно, означает, что p-примарная компонента этой группы равна нулю.

Следствие. *Если* $\operatorname{cd}(G) \leqslant n$ *и группа* A *из* $\mathscr{C}_G$ *является* p*-делимой, то* $H^q(G, A) = 0$ *при* $q > n$.

3.2. Строгая когомологическая размерность

Сохраним те же предположения и обозначения, что и выше. *Строгой когомологической* p*-размерностью* называется (обозначается через $\operatorname{scd}_p(G)$) нижняя грань целых чисел n, удовлетворяющих условию

(**) Для всякого G-модуля $A \in \mathscr{C}_G$ и целого $q > n$ имеет место равенство $H^q(G, A)(p) = 0$.

[В отличие от условия (*) здесь не предполагается, что A должен быть периодическим модулем.]

Положим также $\operatorname{scd}(G) = \sup \operatorname{scd}_p(G)$, $\operatorname{scd}(G)$ называется *строгой когомологической размерностью* группы G.

Предложение 13. *Размерность* $\operatorname{scd}_p(G)$ *равна* $\operatorname{cd}_p(G)$ *или* $\operatorname{cd}_p(G) + 1$.

Очевидно, что $\operatorname{scd}_p(G) \geqslant \operatorname{cd}_p(G)$. Достаточно, следовательно, показать, что $\operatorname{scd}_p(G) \leqslant \operatorname{cd}_p(G) + 1$. Пусть $A \in \mathscr{C}_G$. Рассмотрим каноническое разложение морфизма p: $A \to A$. Оно состоит из двух точных последовательностей

$$0 \to N \to A \to I \to 0,$$

$$0 \to I \to A \to Q \to 0,$$

где $N = A_p$, $I = pA$, $Q = A/pA$, а композиция $A \to I \to A$ является умножением на p.

Пусть $q > \operatorname{cd}_p(G) + 1$. Так как N и Q суть p-примарные периодические группы, то $H^q(G, N) = H^{q-1}(G, Q) = 0$. Поэтому гомоморфизмы

$$H^q(G, A) \to H^q(G, I) \text{ и } H^q(G, I) \to H^q(G, A)$$

инъективны. Следовательно, умножение на p инъективно в $H^q(G, A)$; это означает, что $H^q(G, A)(p)=0$. Таким образом, $\mathrm{scd}_p(G) \leqslant \mathrm{cd}_p(G)+1$, что и требовалось доказать.

Примеры. (1) Положим $G=\hat{\mathbf{Z}}$. Тогда $\mathrm{cd}_p(G)=1$ для каждого простого числа p (это доказывается легко, см., например, [CL], стр. 197, предложение 2)[1]). С другой стороны, группа $H^2(G, \mathbf{Z})$ изоморфна группе $H^1(G, \mathbf{Q}/\mathbf{Z})=\mathbf{Q}/\mathbf{Z}$, отсюда получаем, что $\mathrm{scd}_p(G)=2$.

(2) Пусть $p \neq 2$ и G — группа аффинных преобразований $x \to ax+b$, $b \in \mathbf{Z}_p$, $a \in U_p$ (U_p — группа единиц кольца $\mathbf{Z}_p$). Можно показать, что $\mathrm{cd}_p(G)=\mathrm{scd}_p(G)=2$ (см. гл. II).

(3) Пусть l — простое число и G_l — группа Галуа алгебраического замыкания $\overline{\mathbf{Q}}_l$ поля l-адических чисел $\mathbf{Q}_l$. Тейт показал, что $\mathrm{cd}_p(G_l)=\mathrm{scd}_p(G_l)=2$ для любого p.

Упражнение. Показать, что размерность $\mathrm{scd}_p(G)$ не может быть равной 1.

---

[1]) На основании предложения 11 достаточно доказать, что $H^2(\hat{\mathbf{Z}}, A)=0$, где A — простой дискретный $\hat{\mathbf{Z}}$-модуль, аннулируемый умножением на p. Очевидно, что модуль A конечен ($\hat{\mathbf{Z}}$-орбита каждого элемента $a \in A$ конечна). Далее поскольку

$$H^2(\hat{\mathbf{Z}}, A)=\varinjlim H^2\left(\hat{\mathbf{Z}}/n\hat{\mathbf{Z}}, A^{n\hat{\mathbf{Z}}}\right)$$

и

$$H^2\left(\hat{\mathbf{Z}}/n\hat{\mathbf{Z}}, A^{n\hat{\mathbf{Z}}}\right) \simeq A^{\hat{\mathbf{Z}}}/\mathrm{Norm}\, A^{n\hat{\mathbf{Z}}}$$

(как когомологии конечной циклической группы $\hat{\mathbf{Z}}/n\hat{\mathbf{Z}}$), то имеем

$$H^2(\hat{\mathbf{Z}}, A)=\varinjlim A^{\hat{\mathbf{Z}}}/\mathrm{Norm}\, A^{n\hat{\mathbf{Z}}},$$

где в индуктивной системе для любого целого $m \geqslant 1$ гомоморфизм $A^{\hat{\mathbf{Z}}}/\mathrm{Norm}\, A^{n\hat{\mathbf{Z}}} \to A^{\hat{\mathbf{Z}}}/\mathrm{Norm}\, A^{mn\hat{\mathbf{Z}}}$ индуцирован умножением на m. Таким образом, если m делится на p, то этот гомоморфизм нулевой и, следовательно, $\varinjlim A^{\hat{\mathbf{Z}}}/\mathrm{Norm}\, A^{n\hat{\mathbf{Z}}}=0$, т. е. $H^2(\hat{\mathbf{Z}}, A)=0$. — *Прим. перев.*

3.3. Когомологическая размерность подгрупп и расширений групп

Предложение 14. *Пусть H — замкнутая подгруппа проконечной группы G. Тогда*

$$\mathrm{cd}_p(H) \leqslant \mathrm{cd}_p(G),$$
$$\mathrm{scd}_p(H) \leqslant \mathrm{scd}_p(G).$$

Равенство имеет место в следующих двух случаях:
(i) *индекс $(G:H)$ взаимно прост с p;*
(ii) *подгруппа H открыта в G и $\mathrm{cd}_p(G) < +\infty$.*

Мы рассмотрим только cd_p, для scd_p рассуждения совершенно аналогичны. Если A — дискретный периодический H-модуль, то $M_G^H(A)$ является дискретным периодическим G-модулем и $H^q(G, M_G^H(A)) = H^q(H, A)$. Отсюда очевидным образом следует неравенство

$$\mathrm{cd}_p(H) \leqslant \mathrm{cd}_p(G).$$

Обратное неравенство в случае (i) получается из того, что гомоморфизм Res инъективен на p-примарной компоненте (следствие предложения 9). В случае (ii) положим $n = \mathrm{cd}_p(G)$ и пусть A — дискретный периодический G-модуль, такой, что $H^n(G, A)(p) \neq 0$. Мы хотим показать, что $H^n(H, A)(p) \neq 0$, откуда, конечно, будет следовать, что $\mathrm{cd}_p(H) = n$. Для этого достаточно доказать следующую лемму:

Лемма 4. *Гомоморфизм* Cor: $H^n(H, A) \to H^n(G, A)$ *сюръективен на p-примарных компонентах.*

Действительно, пусть $A^* = M_G^H(A)$ и $\pi\colon A^* \to A$ — гомоморфизм, определенный в п. 2.5 (б). Гомоморфизм π сюръективен и его ядро B является периодическим модулем. Следовательно, $H^{n+1}(G, B)(p) = 0$; это означает, что гомоморфизм

$$H^n(G, A^*) \to H^n(G, A)$$

сюръективен на p-примарных компонентах. Поскольку его можно отождествить с гомоморфизмом коограничения (см. п. 2.5), лемма доказана.

Следствие 1. *Пусть* G_p — *силовская* p-*подгруппа группы* G; *тогда* $\mathrm{cd}_p(G) = \mathrm{cd}_p(G_p) = \mathrm{cd}(G_p)$ *и* $\mathrm{scd}_p(G) = \mathrm{scd}_p(G_p) = \mathrm{scd}(G_p)$.

Доказательство очевидно.

Следствие 2. *Для того чтобы* $\mathrm{cd}_p(G) = 0$, *необходимо и достаточно, чтобы порядок группы* G *был взаимно прост с* p.

Достаточность очевидна. Для доказательства необходимости можно считать, что G — про-p-группа (см. следствие 1). Если $G \neq \{1\}$, то существует непрерывный гомоморфизм группы G на $\mathbf{Z}/p\mathbf{Z}$. Это следует из элементарных свойств p-групп (см., например, [CL], стр. 146)[1]). Поэтому $H^1(G, \mathbf{Z}/p\mathbf{Z}) \neq 0$, откуда $\mathrm{cd}_p(G) \geqslant 1$.

Следствие 3. *Если* $\mathrm{cd}_p(G) \neq 0, \infty$, *то степень* p, *входящая в порядок группы* G, *бесконечна.*

Здесь также можно предполагать, что G есть про-p-группа. Если бы G была конечна, то из части (ii) предыдущего предложения следовало бы, что $\mathrm{cd}_p(G) = \mathrm{cd}_p(\{1\}) = 0$ в противоречие с предположением. Следовательно, группа G бесконечна.

Следствие 4. *Предположим, что* $\mathrm{cd}_p(G) = n < \infty$. *Для справедливости равенства* $\mathrm{scd}_p(G) = n$ *необходимо и достаточно, чтобы выполнялось следующее условие:* $H^{n+1}(H, \mathbf{Z})(p) = 0$ *для любой открытой подгруппы* H *из* G.

---

[1]) Каждая конечная p-группа G обладает композиционным рядом

$$\{1\} = G_n \subset G_{n-1} \subset \ldots \subset G_0 = G,$$

где G_i — нормальные делители в G, $G_i/G_{i+1} = \mathbf{Z}/p\mathbf{Z}$, а p^n — порядок группы G. Это непосредственно следует из известной теоремы: центр нетривиальной p-группы нетривиален. Вот короткое доказательство: действие G на себе внутренними автоморфизмами разбивает ее на орбиты, число элементов в каждой из которых либо равно 1, либо делится на p. Отсюда уже следует утверждение, поскольку порядок G есть степень p. — *Прим. перев.*

Условие, очевидно, необходимо. Обратно, если оно выполнено, то $H^{n+1}(G, A)(p)=0$ для всякого дискретного G-модуля A вида $M_G^H(\mathbf{Z})$. Но каждый дискретный G-модуль B конечного типа над $\mathbf{Z}$ изоморфен некоторому фактормодулю A/C модуля такого вида (за H следует взять открытый нормальный делитель в G, действующий тривиально на B). Поскольку $H^{n+2}(G, C)(p)=0$, из этого следует, что $H^{n+1}(G, B)(p)=0$. С помощью предельного перехода этот результат распространяется на произвольные дискретные G-модули, что и требовалось доказать.

[Пусть H — открытая подгруппа проконечной группы G и p — простое число. Предположим, что $\mathrm{cd}_p(H)<\infty$. В силу предложения 14

$$\mathrm{cd}_p(G)=\mathrm{cd}_p(H) \quad \text{или} \quad \mathrm{cd}_p(G)=\infty.$$

Можно показать, что второй случай представляется только, если G содержит элемент порядка p: в доказательстве существенно используются операции Стинрода. См. Серр [5*].]

Предложение 15. *Пусть H — замкнутый нормальный делитель проконечной группы G. Тогда имеет место неравенство*

$$\mathrm{cd}_p(G)\leqslant \mathrm{cd}_p(H)+\mathrm{cd}_p(G/H).$$

Воспользуемся спектральной последовательностью расширений групп

$$E_2^{i,j}=H^i\big(G/H, H^j(H, A)\big)\Rightarrow H^n(G, A).$$

Пусть A — дискретный периодический G-модуль. Возьмем

$$n>\mathrm{cd}_p(H)+\mathrm{cd}_p(G/H).$$

Если $i+j=n$, то либо $i>\mathrm{cd}_p(G/H)$, либо $j>\mathrm{cd}_p(H)$. В каждом из этих случаев p-примарная компонента группы $E_2^{i,j}$ равна нулю, откуда следует, что равна нулю и p-примарная компонента группы $H^n(G, A)$. Предложение доказано.

Замечание. Предположим, что $n = \mathrm{cd}_p(H)$ и $m = \mathrm{cd}_p(G/H)$ конечны. Тогда спектральная последовательность обеспечивает канонический изоморфизм

$$H^{n+m}(G, A)(p) = H^m\big(G/H, H^n(H, A)\big)(p).$$

Этот изоморфизм позволяет дать условие того, чтобы $\mathrm{cd}_p(G)$ равнялось сумме $\mathrm{cd}_p(G/H) + \mathrm{cd}_p(H)$, см. § 4.

Упражнения. 1) Показать, что в утверждении (ii) предложения 14 предположение „H открыта в G“ можно заменить на следующее: „степень p в индексе $(G:H)$ конечна“.

2) Сохраняя условия предложения 15, предположим, кроме того, что степень p в индексе $(G:H)$ не равна нулю (т. е. $\mathrm{cd}_p(G/H) \neq 0$). Показать, что тогда справедливо неравенство

$$\mathrm{scd}_p(G) \leqslant \mathrm{cd}_p(H) + \mathrm{scd}_p(G/H).$$

3) Пусть n — целое число. Предположим, что p-примарные компоненты групп $H^{n+1}(H, \mathbf{Z})$ и $H^{n+2}(H, \mathbf{Z})$ равны нулю для каждой открытой подгруппы H из G. Показать, что в этом случае $\mathrm{scd}_p(G) \leqslant n$. [Пусть G_p — силовская p-подгруппа в G; следует доказать, что $H^{n+1}(G_p, \mathbf{Z}/p\mathbf{Z}) = 0$, и применить результат § 4 для доказательства неравенства $\mathrm{cd}_p(G) \leqslant n$.]

3.4. Характеризация проконечных групп G, для которых $\mathrm{cd}_p(G) \leqslant 1$

Пусть $1 \to P \to E \xrightarrow{\pi} W \to 1$ — некоторое расширение проконечных групп. Мы говорим, что проконечная группа G обладает *свойством поднятия* относительно предыдущего расширения, если всякий морфизм $f\colon G \to W$ поднимается до морфизма $f'\colon G \to E$ (т. е. существует морфизм f', такой, что $f = \pi \circ f'$). Это эквивалентно тому, что расширение

$$1 \to P \to E_f \to G \to 1,$$

обратный образ E относительно f[1]), является тривиальным.

Предложение 16. *Пусть G — проконечная группа и p — простое число. Тогда эквивалентны следующие свойства:*

(i) $\mathrm{cd}_p(G) \leqslant 1$;

(ii) *группа G обладает свойством поднятия относительно тех расширений $1 \to P \to E \to W \to 1$, в которых E — конечная группа, а P — абелева p-группа, аннулируемая умножением на p;*

(ii′) *всякое расширение группы G с помощью конечной абелевой p-группы, аннулируемой умножением на p, является тривиальным;*

(iii) *группа G обладает свойством поднятия относительно расширений $1 \to P \to E \to W \to 1$, где P — любая про-p-группа;*

(iii′) *всякое расширение группы G с помощью про-p-группы является тривиальным.*

(Речь идет, конечно, о расширениях в категории проконечных групп.)

Очевидно, что (iii)$\Leftrightarrow$(iii′) и что (ii′)$\Rightarrow$(ii). Для доказательства импликации (ii)$\Rightarrow$(ii′) рассмотрим произвольное расширение

$$1 \to P \to E_0 \to G \to 1$$

группы G с помощью конечной абелевой p-группы P, аннулируемой умножением на p. В силу леммы 2 п. 1.2 это расширение тривиально над некоторой открытой подгруппой H в G, которую можно считать нормальным делителем. Это означает, что рассматриваемое расширение

[1]) Пусть $0 \to A \to C \to B \to 0$ — точная последовательность групп (расширение B с помощью A) и $f\colon B' \to B$ — некоторый гомоморфизм. Обратным образом этой последовательности относительно f называется точная последовательность

$$0 \to A \to C_f \to B' \to 0,$$

где C_f определяется как подгруппа в прямом произведении $C \times B'$, состоящая из таких пар $c \times b'$, компоненты которых проектируются при гомоморфизмах $C \to B$ и $B' \to B$ в один и тот же элемент. Иначе говоря, C_f является расслоенным произведением C и B' над B. — *Прим. перев.*

является обратным образом расширения E группы G/H с помощью группы P. Применяя условие (ii) к этому последнему расширению, находим, что G „поднимается“ в (E), откуда следует утверждение (ii′).

Соответствие между элементами группы $H^2(G, A)$ и классами расширений группы G с помощью A (см. п. 2.3) показывает, что (i)$\Leftrightarrow$(ii′). Импликация (iii′)$\Rightarrow$(ii′) — тривиальна. Осталось, таким образом, доказать, что условие (ii′) влечет за собой (iii′). Для этого сошлемся на следующую лемму:

Лемма 5. *Пусть H — замкнутый нормальный делитель проконечной группы E и H' — открытая подгруппа в H. Тогда существует открытая подгруппа H'' в H, которая содержится в H' и является нормальным делителем в группе E.*

Пусть N — нормализатор подгруппы H' в E, т. е. множество элементов $x \in E$, таких, что $xH'x^{-1} = H'$. Так как $xH'x^{-1}$ содержится в H, то N, очевидно, представляет собой множество элементов, которые отображают некоторый компакт (а именно, H') в открытое множество (H', рассматриваемое как подпространство в H). Отсюда заключаем, что N само открыто, следовательно, подгруппа H' имеет только конечное число сопряженных с ней подгрупп. Их пересечение H'' отвечает всем требуемым условиям.

Возвратимся к доказательству импликации (ii′)$\Rightarrow$(iii′). Пусть $1 \to P \to E \to G \to 1$ — расширение группы G с помощью про-p-группы P. Обозначим через X множество пар (P', s), где P' — открытая подгруппа в P, являющаяся нормальным делителем в группе E, и s — „поднятие“ группы G в расширении

$$1 \to P/P' \to E/P' \to G \to 1.$$

Множество X очевидным способом упорядочено и индуктивно. Пусть (P', s) — максимальный элемент в X; тогда $P' = \{1\}$ (что доказывает (iii′)). Действительно, при необходимости факторизуя по P', мы можем предполагать, что максимальным является элемент (P, id); надо показать тогда, что $P = \{1\}$. В противном случае на основании леммы 5 должна существовать некоторая собственная подгруппа P', открытая в P и являющаяся нормальным делителем в G. Исполь-

зуя метод „отвинчивания“, можно предполагать, что P/P' является абелевой p-группой, аннулируемой умножением на p. В силу условия (ii′) расширение

$$1 \to P/P' \to E/P' \to G \to 1$$

будет тогда тривиальным в противоречие с максимальностью (P, id), что и требовалось доказать.

Следствие. *Свободная про-p-группа $F(I)$ имеет когомологическую размерность, не превосходящую* 1.

Проверим, например, свойство (iii′). Пусть $E/P = G$ — какое-нибудь расширение группы $G = F(I)$ с помощью про-p-группы P и x_i — канонические образующие группы $F(I)$. Пусть $s\colon G \to E$ — некоторое непрерывное сечение, проходящее через единичный элемент в E (см. предложение 1), и пусть $e_i = s(x_i)$. Поскольку x_i стремятся к 1, то то же самое верно и для e_i. Из предложения 5 следует тогда существование морфизма $u\colon G \to E$, для которого $u(x_i) = e_i$. Следовательно, расширение E тривиально, что и требовалось доказать.

Упражнения. 1) Пусть G — проконечная группа и p — простое число. Рассмотрим следующее свойство:

$(*_p)$ Для всякого расширения $1 \to P \to E \to W \to 1$, где E — конечная группа, а P — про-p-группа, и для всякого *сюръективного* морфизма

$$f\colon G \to W$$

существует *сюръективный* морфизм $f'\colon G \to E$, поднимающий морфизм f.

(a) Показать, что это свойство эквивалентно объединению двух следующих:

(1_p) $\mathrm{cd}_p(G) \leqslant 1$;

(2_p) для каждого открытого нормального делителя U в G и для каждого целого $N \geqslant 0$ существуют $z_1, \ldots, z_N \in H^1(U, \mathbf{Z}/p\mathbf{Z})$, такие, что элементы $s(z_i)$ $(s \in G/U, 1 \leqslant i \leqslant N)$ линейно независимы над $\mathbf{Z}/p\mathbf{Z}$.

[Начать с доказательства достаточности условия $(*_p)$ в следующих двух случаях: (i) каждая подгруппа в E, проектирующаяся на все W, равна E; (ii) группа E является полупрямым произведением группы W на группу P и

P — абелева про-p-группа, аннулируемая умножением на p. Условие (i) эквивалентно (1_p), условие (ii) — условию (2_p).]

(б) Показать, что для проверки условия (2_p) достаточно рассматривать сколь угодно малые подгруппы U (т. е. содержащиеся в любой наперед заданной открытой подгруппе).

2) (а) Пусть G и G' — две проконечные группы, удовлетворяющие условию $(*_p)$ для любого p. Предположим, что существует база (G_n) $\left(\text{соответственно } (G'_n)\right)$ окрестностей единицы в G (соответственно G'), образованная открытыми нормальными делителями, такими, что для каждого n факторгруппы G/G_n $\left(\text{соответственно } G'/G'_n\right)$ разрешимы. Показать, что тогда G и G' изоморфны.

[Построить с помощью индукции по n две убывающие последовательности (H_n) и (H'_n), где $H_n \subset G_n$, $H'_n \subset G'_n$ и H_n, H'_n — открытые нормальные делители в G и G' соответственно, и согласованную последовательность (f_n) изоморфизмов $G/H_n \to G'/H'_n$.]

(б) Пусть L — свободная группа (неабелева), порожденная счетным семейством элементов (x_i). Положим $\hat{L} = \varprojlim L/N$, где N пробегает нормальные делители из L, содержащие почти все x_i и такие, что L/N — конечные разрешимые группы. Показать, что $\hat{L}$ — метризуемая проразрешимая группа (т. е. проективный предел разрешимых конечных групп), которая удовлетворяет условию $(*_p)$ для любого p. Используя (а), показать, что всякая проконечная группа, обладающая этими свойствами, изоморфна $\hat{L}$.

(См. Ивасава [1].)

3.5. Дуализирующие модули

Пусть G — проконечная группа. Через $\mathscr{C}_G^f$ (соответственно $\mathscr{C}_G^t$) мы обозначаем категорию конечных дискретных G-модулей A (соответственно периодических G-модулей). Категория $\mathscr{C}_G^t$ отождествляется с категорией $\varinjlim \mathscr{C}_G^f$ индуктивных пределов объектов из $\mathscr{C}_G^f$.

Обозначим через (Ab) категорию абелевых групп. Для всякого объекта $M \in (\mathrm{Ab})$ положим $M^* = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$

и снабдим эту группу топологией поточечной сходимости функций ($\mathbf{Q}/\mathbf{Z}$ рассматривается как дискретная группа). Если M — периодическая группа (соответственно конечная группа), то M^* компактна (соответственно конечна). Таким образом устанавливается некоторая эквивалентность между категорией абелевых периодических групп и двойственной категорией к категории абелевых компактных проконечных групп („двойственность Понтрягина“).

Предложение 17. *Пусть n — целое число; предположим, что*

(а) $\operatorname{cd}(G) \leqslant n$;

(б) *для каждого* $A \in \mathcal{C}_G^f$ *группа* $H^n(G, A)$ *конечна. Тогда функтор* $H^n(G, A)^*$ *представляется в* $\mathcal{C}_G^f$ *некоторым объектом* $I \in \mathcal{C}_G^t$.

[Другими словами, существует объект $I \in \mathcal{C}_G^t$, такой, что функторы $\operatorname{Hom}_G(A, I)$ и $H^n(G, A)^*$ изоморфны; модуль A пробегает категорию $\mathcal{C}_G^f$.]

Положим $S(A) = H^n(G, A)$ и $T(A) = H^n(G, A)^*$. Предположение (а) показывает, что S является ковариантным и точным справа функтором из $\mathcal{C}_G^f$ в (Ab). Из предположения (б) следует, что его значения принадлежат подкатегории (Ab^f) категории (Ab), образованной *конечными* группами. Так как функтор $*$ точен, то из этого следует, что T — контравариантный и точный слева функтор из $\mathcal{C}_G^f$ в (Ab). Предложение 17 вытекает в таком случае из следующей леммы:

Лемма 6. *Пусть $\mathcal{C}$ — нётерова абелева категория*[1]) *и* $T\colon \mathcal{C}^0 \to (\mathrm{Ab})$ — *контравариантный и точный справа функтор из $\mathcal{C}$ в* (Ab). *Тогда T представляется некоторым объектом I в* $\varinjlim \mathcal{C}$.

Этот результат содержится в докладе Гротендика на семинаре Бурбаки (доклад 195, стр. 195-06), а также в диссертации Габриэля (гл. II, п. 4)[2]). Мы напомним принцип доказательства Гротендика.

---

[1]) Категория $\mathcal{C}$ называется нётеровой, если для любого объекта из $\mathcal{C}$ выполняется условие обрыва возрастающих цепочек подобъектов. — *Прим. перев.*

[2]) См. Габриэль [1]. — *Прим. перев.*

Пару (A, x), $A \in \mathscr{C}$, $x \in T(A)$, назовем *минимальной*, если x не принадлежит никакому $T(B)$, где B — факторобъект объекта A, отличный от самого A (если B есть факторобъект объекта A, то $T(B)$ отождествляется с подгруппой в группе $T(A)$). Пусть (A', x') и (A, x)—минимальные пары. Будем говорить, что пара (A', x') *больше*, чем пара (A, x), если существует морфизм u: $A \to A'$, такой, что $T(u)(x') = x$ (в этом случае проверяется, что u единствен). Множество минимальных пар является, таким образом, упорядоченным и фильтрующимся. Положим $I = \varinjlim A$, предел берется по этому отношению порядка. Положим $T(I) = \varprojlim T(A)$; элементы x определят некоторый канонический элемент $i \in T(I)$. Пусть f: $A \to I$ — произвольный морфизм. Ставя в соответствие морфизму f элемент $T(f)(i)$ в $T(A)$, получаем гомоморфизм группы $\mathrm{Hom}(A, I)$ в группу $T(A)$. Без труда проверяется (здесь надо воспользоваться предположением нётеровости), что построенный гомоморфизм является изоморфизмом.

Замечания. 1. В нашем случае $T(I)$ — просто двойственная (компактная) группа к периодической группе $H^n(G, I)$ и канонический элемент $i \in T(I)$ — некоторый гомоморфизм

$$i\colon H^n(G, I) \to \mathbf{Q}/\mathbf{Z}.$$

Отображение $\mathrm{Hom}_G(A, I) \to H^n(G, A)^*$ получается сопоставлением каждому $f \in \mathrm{Hom}_G(A, I)$ гомоморфизма

$$H^n(G, A) \xrightarrow{f} H^n(G, I) \xrightarrow{i} \mathbf{Q}/\mathbf{Z}.$$

2. Модуль I называется *дуализирующим* модулем для группы G (в размерности n). Он определен с точностью до изоморфизма; вернее, *однозначно с точностью до изоморфизма определена пара* (I, i).

3. Если ограничиваться только p-примарными G-модулями, то достаточно одного условия $\mathrm{cd}_p(G) \leqslant n$.

4. Переходя к пределу, используя предложение 17, получаем, что если $A \in \mathscr{C}_G^t$, то группа $H^n(G, A)$ двойственна компактной группе $\mathrm{Hom}_G(A, I)$ с топологией простой сходимости. Если положить $\tilde{A} = \mathrm{Hom}(A, I)$ и рассмотреть $\tilde{A}$ как G-модуль, где действие группы G задается

формулой $(gf)(a) = gf(g^{-1}a)$, то получим, что $\mathrm{Hom}_G(A, I) = H^0(G, \tilde{A})$, и предложение 17 выражает тогда просто *двойственность* между группами $H^n(G, A)$ и $H^0(G, \tilde{A})$, первая из которых дискретна, а вторая компактна.

Предложение 18. *Пусть I — дуализирующий модуль для группы G, тогда он является также дуализирующим модулем для любой открытой подгруппы H из G.*

Если $A \in \mathscr{C}_H^f$, то $M_G^H(A) \in \mathscr{C}_G^f$ и $H^n(G, M_G^H(A)) = H^n(H, A)$. Отсюда получаем, что группа $H^n(H, A)$ двойственна группе $\mathrm{Hom}_G(M_G^H(A), I)$. Но легко видеть, что последняя группа функториально отождествляется с группой $\mathrm{Hom}_H(A, I)$. Это означает, что I является дуализирующим модулем для H.

Замечание. Каноническое вложение $\mathrm{Hom}_G(A, I)$ в $\mathrm{Hom}(A, I)$ определяет двойственный сюръективный гомоморфизм $H^n(H, A) \to H^n(G, A)$, который совпадает с гомоморфизмом *кoограничения*. Это видно из интерпретации коограничения, указанной в п. 2.5.

Следствие. *Пусть $A \in \mathscr{C}_G^f$. Тогда группа $\tilde{A} = \mathrm{Hom}(A, I)$ является индуктивным пределом групп, двойственных к группам $H^n(H, A)$, где H пробегает множество всех открытых подгрупп группы G (а отображения двойственны к коограничениям).*

Этот результат получается по двойственности из очевидной формулы

$$\tilde{A} = \varinjlim \mathrm{Hom}_H(A, I).$$

Замечание. Можно уточнить предыдущий результат, показав, что действие группы G на $\tilde{A}$ получается из естественных действий факторгрупп G/H на $H^n(H, A)$ с помощью предельного перехода по всем открытым нормальным делителям H в G.

Предложение 19. *Предположим, что $n \geqslant 1$. Для того чтобы выполнялось равенство $\mathrm{scd}_p(G) = n + 1$, необходимо и достаточно, чтобы существовала такая открытая подгруппа H группы G, что группа I^H содержит подгруппу, изоморфную $\mathbf{Q}_p/\mathbf{Z}_p$.*

Утверждение „I^H содержит подгруппу, изоморфную $\mathbf{Q}_p/\mathbf{Z}_p$“ эквивалентно тому, что $\operatorname{Hom}_H(\mathbf{Q}_p/\mathbf{Z}_p, I) \neq 0$ или также тому, что $H^n(H, \mathbf{Q}_p/\mathbf{Z}_p) \neq 0$. Но группа $H^n(H, \mathbf{Q}_p/\mathbf{Z}_p)$ является p-примарной компонентой группы $H^n(H, \mathbf{Q}/\mathbf{Z})$, которая изоморфна группе $H^{n+1}(H, \mathbf{Z})$ (следует использовать обычную точную последовательность

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

и предположение, что $n \geqslant 1$). Предложение получается теперь из следствия 4 предложения 14.

Примеры. (1) Возьмем $G = \hat{\mathbf{Z}}$ и $n = 1$. Пусть $A \in \mathscr{C}_G^t$. Обозначим через σ автоморфизм группы A, определяемый канонической образующей группы G. Легко проверить (см. [CL], стр. 197), что $H^1(G, A)$ отождествляется с $A_G = A/(\sigma - 1)A$ [1]). Отсюда получаем, что дуализирующим модулем для группы G является модуль $\mathbf{Q}/\mathbf{Z}$ с тривиальным действием G. В частности, это доставляет новое доказательство того, что $\operatorname{scd}_p(G) = 2$ для любого p.

(2) Пусть $\overline{\mathbf{Q}}_l$ — алгебраическое замыкание поля l-адических чисел $\mathbf{Q}_l$ и G — группа Галуа поля $\overline{\mathbf{Q}}_l$ над $\mathbf{Q}_l$. Тогда $\operatorname{cd}(G) = 2$ и соответствующий дуализирующий модуль есть группа μ всех корней из единицы (Тейт). Предыдущее предложение вновь доказывает, что $\operatorname{scd}_p(G) = 2$ для любого p.

§ 4. КОГОМОЛОГИИ ПРО-p-ГРУПП

4.1. Простые модули

Предложение 20. *Пусть G — про-p-группа. Всякий простой дискретный G-модуль, аннулируемый умножением на p, изоморфен $\mathbf{Z}/p\mathbf{Z}$ (с тривиальным действием G).*

---

[1]) Изоморфизм $H^1(\hat{\mathbf{Z}}, A) \to A/(\sigma - 1)A$ получается сопоставлением каждому одномерному коциклу $\varphi\colon \hat{\mathbf{Z}} \to A$ класса $\varphi(1)$ в $A/(\sigma - 1)A$. Вспомнив определение H^1 для циклической группы и переходя к пределу, так же как и в примечании, мы устанавливаем требуемый изоморфизм. При этом существенно используется предположение, что $\hat{\mathbf{Z}}$-модуль A является периодическим. — *Прим. перев.*

Пусть A — такой модуль. Очевидно, что он конечен и его можно рассматривать как G/U-модуль для некоторого подходящего открытого нормального делителя U. Можно также свести все к случаю, когда G является p-группой (конечной), который хорошо известен (см., например, [CL], стр. 146)[1].

Следствие. *Всякий р-примарный конечный дискретный G-модуль обладает композиционным рядом, последовательные факторы которого изоморфны* $\mathbf{Z}/p\mathbf{Z}$.

Доказательство очевидно.

Предложение 21. *Пусть G является про-р-группой и n — целое число. Для того чтобы* $\mathrm{cd}(G) \leqslant n$, *необходимо и достаточно, чтобы* $H^{n+1}(G, \mathbf{Z}/p\mathbf{Z}) = 0$.

Это вытекает из предложений 11 и 20.

Следствие. *Предположим, что размерность* $\mathrm{cd}(G)$ *равна n. Пусть A — конечный дискретный G-модуль, который р-примарен и отличен от нуля. Тогда* $H^n(G, A) \neq 0$.

Действительно, как показывает следствие предложения 20, существует сюрьективный гомоморфизм $A \to \mathbf{Z}/p\mathbf{Z}$. Поскольку $\mathrm{cd}(G) \leqslant n$, то соответствующий гомоморфизм

$$H^n(G, A) \to H^n(G, \mathbf{Z}/p\mathbf{Z})$$

также является сюръективным. Но предложение 21 показывает, что $H^n(G, \mathbf{Z}/p\mathbf{Z}) \neq 0$, откуда и следует утверждение.

---

[1]) Если G является p-группой и A — конечный G-модуль, аннулируемый умножением на p, то A содержит в качестве подмодуля модуль $\mathbf{Z}/p\mathbf{Z}$ с тривиальным действием G. Это устанавливается с помощью рассуждения, уже приведенного в примечании на стр. 28. Пусть $a \in A$ — ненулевой элемент. Рассмотрим подмодуль $A' \subset A$, порожденный элементами $s \cdot a$, $s \in G$. Так как число элементов A' делится на p и существует по крайней мере один G-инвириантный элемент $0 \in A'$, то должен существовать и отличный от нуля G-инвариантный элемент $a' \in A'$ (поскольку число элементов каждой G-орбиты или равно 1, или делится на p). Подмодуль, порожденный a', изоморфен $\mathbf{Z}/p\mathbf{Z}$. Таким образом, если модуль A прост, то он имеет вид $\mathbf{Z}/p\mathbf{Z}$. — *Прим. перев.*

Следующее предложение является уточнением предложения 15:

Предложение 22. *Пусть G — проконечная группа и H — замкнутый нормальный делитель в G. Предположим, что $n = \mathrm{cd}_p(H)$ и $m = \mathrm{cd}_p(G/H)$ конечны. Тогда равенство*

$$\mathrm{cd}_p(G) = n + m$$

достигается в каждом из следующих двух случаев:

(i) *H является про-p-группой, и группа $H^n(H, \mathbf{Z}/p\mathbf{Z})$ конечна;*

(ii) *H содержится в центре группы G.*

Пусть $(G/H)'$ — силовская p-подгруппа в группе G/H и G' — ее полный прообраз в G. Тогда $\mathrm{cd}_p(G') \leqslant \mathrm{cd}_p(G) \leqslant n + m$ и $\mathrm{cd}_p(G'/H) = m$. Достаточно, следовательно, доказать, что $\mathrm{cd}_p(G') = n + m$, иначе говоря, можно считать, что G/H — про-p-группа. С другой стороны (см. п. 3.3),

$$H^{n+m}(G, \mathbf{Z}/p\mathbf{Z}) = H^m(G/H, H^n(H, \mathbf{Z}/p\mathbf{Z})).$$

В случае (i) группа $H^n(H, \mathbf{Z}/p\mathbf{Z})$ конечна и отлична от нуля (предложение 21). Отсюда следует, что группа $H^m(G/H, H^n(H, \mathbf{Z}/p\mathbf{Z}))$ отлична от нуля (следствие предложения 21), откуда $H^{n+m}(G, \mathbf{Z}/p\mathbf{Z}) \neq 0$ и $\mathrm{cd}_p(G) = n + m$. В случае (ii) группа H абелева, следовательно, она равна прямому произведению своих силовских подгрупп H_l. Из предложения 21 следует, что $H^n(H_p, \mathbf{Z}/p\mathbf{Z}) \neq 0$. С другой стороны, действие факторгруппы G/H на $H^n(H, \mathbf{Z}/p\mathbf{Z})$ тривиально. В самом деле, в случае произвольной группы $H^n(H, A)$ это действие возникает из действия G на H (внутренними автоморфизмами) и действия G на A (см. [CL], стр. 124). В рассматриваемом случае оба эти действия тривиальны. Таким образом, G/H-модуль $H^n(H, \mathbf{Z}/p\mathbf{Z})$ изоморфен некоторой прямой сумме $(\mathbf{Z}/p\mathbf{Z})^{(I)}$, где множество индексов I непусто. Следовательно, имеют место соотношения

$$H^{n+m}(G, \mathbf{Z}/p\mathbf{Z}) = H^m(G/H, \mathbf{Z}/p\mathbf{Z})^{(I)} \neq 0,$$

что завершает доказательство.

Упражнение. Предположим, что G является про-p-группой и что для каждого i группа $H^i(G, \mathbf{Z}/p\mathbf{Z})$ имеет

конечную размерность n_i над $\mathbf{Z}/p\mathbf{Z}$ и $n_i=0$ для всех достаточно больших чисел i (т. е. $\operatorname{cd}(G)<+\infty$). Положим $E(G)=\sum(-1)^i n_i$ и будем называть *характеристикой Эйлера — Пуанкаре* группы G.

(а) Пусть A — дискретный G-модуль конечного порядка p^a. Показать, что тогда группы $H^i(G, A)$ конечны. Обозначив через $p^{n_i(A)}$ их порядки, положим

$$\chi(A)=\sum(-1)^i n_i(A).$$

Показать, что $\chi(A)=aE(G)$.

(б) Пусть H — открытая подгруппа в G. Показать, что H обладает теми же свойствами, что и G, и имеет место равенство

$$E(H)=(G:H)\,E(G).$$

(в) Пусть $X/N=G$ — расширение группы G с помощью про-p-группы N, для которой выполнены те же условия, что и для G. Показать, что эти условия выполнены также и для X и имеет место равенство

$$E(X)=E(G)\cdot E(N).$$

(г) Пусть G_1 — про-p-группа. Предположим, что существует открытая подгруппа G в G_1, для которой выполнены указанные выше условия. Положим

$$E(G_1)=E(G)/(G_1:\ G).$$

Показать, что это число (не обязательно конечное) не зависит от выбора группы G_1. Обобщить пункты (б) и (в).

4.2. Интерпретация H^1: образующие

Пусть G является про-p-группой. До конца этого параграфа мы полагаем

$$H^i(G)=H^i(G,\ \mathbf{Z}/p\mathbf{Z}).$$

В частности, через $H^1(G)$ обозначается группа $H^1(G, \mathbf{Z}/p\mathbf{Z})= =\operatorname{Hom}(G,\ \mathbf{Z}/p\mathbf{Z})$.

Предложение 23. *Пусть f: $G_1\to G_2$ — морфизм про-p-групп. Для того чтобы f был сюръективным, необходимо и достаточно, чтобы гомоморфизм $H^1(f)$: $H^1(G_2)\to\to H(G_1)$ был инъективным.*

Необходимость очевидна. Обратно, предположим, что $f(G_1) \neq G_2$. Тогда существует конечная факторгруппа P_2 группы G_2, такая, что образ группы $f(G_1)$ в P_2, который мы обозначим через P_1, будет отличен от P_2. Известно (см., например, Холл [1], гл. 12), что в этом случае существует нормальный делитель индекса p в P_2, который содержит P_1. Другими словами, существует ненулевой гомоморфизм $\pi: P_2 \to \mathbf{Z}/p\mathbf{Z}$, отображающий группу P_1 в 0. Рассматривая π как элемент из $H^1(G_2)$, получаем, что $\pi \in \operatorname{Ker} H^1(f)$. Предложение доказано.

Замечание. Пусть G является про-p-группой. Обозначим через G^* подгруппу в G, являющуюся пересечением ядер всех гомоморфизмов $\pi: G \to \mathbf{Z}/p\mathbf{Z}$. Легко видеть, что $G^* = G^p \cdot (G, G)$, где (G, G) обозначает, как обычно, коммутант группы G. Группы G/G^* и $H^1(G)$ двойственны друг другу (первая компактна, вторая дискретна). Предложение 23 можно тогда переформулировать следующим образом.

Предложение 23′. *Для того чтобы морфизм $G_1 \to G_2$ был сюръективен, необходимо и достаточно, чтобы индуцированный им морфизм $G_1/G_1^* \to G_2/G_2^*$ был также сюръективен.*

Группа G^* играет, таким образом, роль „радикала“, и предыдущее предложение является аналогом известной в коммутативной алгебре „леммы Накаямы“.

Пример. Пусть G — свободная группа $F(I)$, определенная в п. 1.5, тогда предложение 5 показывает, что группа $H^1(G)$ отождествляется с прямой суммой $(\mathbf{Z}/p\mathbf{Z})^{(I)}$, а значит, группа G/G^*—с прямым произведением $(\mathbf{Z}/p\mathbf{Z})^I$.

Предложение 24. *Пусть G — про-p-группа и I — некоторое множество. Пусть $\theta: H^1(G) \to (\mathbf{Z}/p\mathbf{Z})^{(I)}$ — некоторый гомоморфизм. Тогда*

(а) *существует морфизм $f: F(I) \to G$, такой, что $\theta = H^1(f)$;*

(б) *если θ инъективен, то f сюръективен;*

(в) *если* θ *биективен и* $\mathrm{cd}(G) \leqslant 1$, *то* f — *изоморфизм.*

По двойственности гомоморфизм θ определяет некоторый морфизм компактных групп θ': $(\mathbf{Z}/p\mathbf{Z})^I \to G/G^*$ и с помощью композиции морфизм $F(I) \to G/G^*$. Так как $F(I)$ обладает свойством поднятия (см. п. 3.4), то существует, следовательно, морфизм $f: F(I) \to G$, что доказывает, очевидно, пункт (а).

Если же θ инъективен, то предложение 23 показывает, что f сюръективен. Если, кроме того, $\mathrm{cd}(G) \leqslant 1$, то из предложения 16 следует существование морфизма $g: G \to F(I)$, такого, что $f \circ g = 1$. Отсюда имеем $H^1(g) \circ H^1(f) = 1$. Если $\theta = H^1(f)$ биективен, то $H^1(g)$ также биективен, следовательно, морфизм g сюръективен. Но так как $f \circ g = 1$, то это означает, что f и g являются изоморфизмами. Доказательство закончено.

Следствие 1. *Для того чтобы про-р-группа G была изоморфна факторгруппе свободной про-р-группы $F(I)$, необходимо и достаточно, чтобы мощность базиса группы $H^1(G)$ была не больше чем* $\mathrm{Card}(I)$.

Действительно, если это условие выполнено, то можно вложить группу $H^1(G)$ в группу $(\mathbf{Z}/p\mathbf{Z})^{(I)}$ и применить пункт (б).

В частности, всякая про-р-группа есть факторгруппа свободной про-р-группы.

Следствие 2. *Для того чтобы про-р-группа была свободной, необходимо и достаточно, чтобы она имела когомологическую размерность, не превосходящую* 1.

Необходимость известна. Обратно, пусть $\mathrm{cd}(G) \leqslant 1$. Выберем некоторый базис $(e_i)_{i \in I}$ в $H^1(G)$ и построим изоморфизм

$$\theta: H^1(G) \to (\mathbf{Z}/p\mathbf{Z})^{(I)}.$$

Тогда, как показывает предложение 24, группа G изоморфна группе $F(I)$.

Укажем два частных случая предыдущего предложения.

Следствие 3. *Всякая замкнутая подгруппа свободной про-р-группы свободна.*

Доказательство очевидно.

Следствие 4. *Про-p-группы $F_s(I)$, определенные в п. 1.5, свободны.*

В самом деле, эти группы удовлетворяют свойству поднятия предложения 16. Следовательно, они имеют когомологическую размерность, не превосходящую 1.

В частном случае, когда множество I конечно, следствие 1 можно уточнить. Пусть $g_1, \ldots, g_n$ — элементы из G. Мы говорим, что g_i *порождают* (топологически) группу G, если порожденная ими (в алгебраическом смысле) подгруппа всюду плотна в G. Это равносильно утверждению, что каждый фактор G/U, где U — открытая подгруппа, порождается образами элементов g_i.

Предложение 25. *Пусть $g_1, \ldots, g_n$ — элементы некоторой про-p-группы G. Тогда эквивалентны следующие условия:*

(а) *элементы $g_1, \ldots, g_n$ порождают группу G,*

(б) *гомоморфизм g: $F(n) \to G$, определенный элементом g_i (см. предложение 5), сюръективен,*

(в) *образы элементов g_i порождают группу G/G^*,*

(г) *всякий гомоморфизм $\pi \in H^1(G)$, аннулирующий все g_i, равен нулю.*

Эквивалентность (а) $\Leftrightarrow$ (б) видна непосредственно (или следует из предложения 24). Эквивалентность (б) $\Leftrightarrow$ (в) следует из предложения 23′, и (в) $\Leftrightarrow$ (г) получаем, используя двойственность между группами $H^1(G)$ и G/G^*.

Следствие. *Минимальное число образующих группы G равно размерности $H^1(G)$.*

Доказательство очевидно.

Определенное таким образом число будем называть рангом группы G.

Упражнения. 1) Показать, что если множество I бесконечно, то $F_s(I)$ изоморфна $F(2^I)$.

2) Для того чтобы про-p-группа G была метризуемой, необходимо и достаточно, чтобы $H^1(G)$ было счетным.

3) Пусть G является про-p-группой. Положим $G_1 = G$ и определим по индукции группы G_n посредством фор-

мулы $G_n = (G_{n-1})^*$. Показать, что G_n образуют убывающую последовательность замкнутых нормальных делителей в группе G, пересечение которых равно $\{1\}$. Показать, что подгруппы G_n открыты тогда и только тогда, когда ранг группы G конечен.

4) Обозначим через $n(G)$ ранг про-p-группы G.

(а) Пусть F — свободная про-p-группа конечного ранга и U — открытая подгруппа F. Показать, что U также является свободной про-p-группой конечного ранга и имеет место равенство

$$n(U) - 1 = (F : U) \cdot (n(F) - 1).$$

[Использовать упражнение в п. 4.1, предварительно заметив, что $E(F) = 1 - n(F)$.]

(б) Пусть G является про-p-группой конечного ранга. Показать, что если подгруппа U открыта в G, то она также имеет конечный ранг. Доказать неравенство

$$n(U) - 1 \leqslant (G : U)(n(G) - 1).$$

[Представить G как факторгруппу свободной про-p-группы F того же ранга и применить пункт (а) к полному прообразу U' группы U в F.]

Показать, что если в этой формуле равенство достигается для всех открытых подгрупп U, то группа G свободна. [Способ тот же, что и выше. Сравнить фильтрации (F_n) и (G_n), определенные в упражнении 3; показать с помощью индукции по n, что проекция $F \to G$ определяет при факторизации изоморфизмы $F/F_n \to G/G_n$. Вывести отсюда, что она сама является изоморфизмом.]

4.3. Интерпретация H^2: соотношения

Пусть F — про-p-группа и R — замкнутый нормальный делитель в F. Пусть $r_1, \ldots, r_n \in R$. Мы говорим, что элементы r_i порождают R (как нормальный делитель в F), если все элементы, сопряженные с r_i, порождают (в алгебраическом смысле) подгруппу, всюду плотную в R. Это равносильно утверждению, что R является наименьшим замкнутым нормальным делителем в F, содержащим все r_i.

Предложение 26. *Для того чтобы элементы r_i порождали R (как нормальный делитель в F), необходимо*

и достаточно, чтобы всякий элемент $\pi \in H^1(R)^{F/R}$, *аннулирующий все* r_i, *был равен нулю.*

[Имеет место равенство $H^1(R) = \mathrm{Hom}(R/R^*, \mathbf{Z}/p\mathbf{Z})$, и факторгруппа F/R действует на R/R^* внутренними автоморфизмами. Следовательно, она действует также и на $H^1(R)$ — частный случай результатов п. 2.6.]

Предположим, что все элементы $g r_i g^{-1}$, сопряженные с r_i, порождают всюду плотную подгруппу в R, а π — такой элемент группы $H^1(R)^{F/R}$, что $\pi(r_i) = 0$ для всех i. Поскольку π инвариантен относительно действия F/R, то $\pi(gxg^{-1}) = \pi(x)$ для всех $g \in F$ и $x \in R$. Отсюда следует, что π аннулирует также $g r_i g^{-1}$ и, значит, все R, откуда $\pi = 0$.

Обратно, предположим, что это условие выполнено, и пусть R' — наименьший замкнутый нормальный делитель в F, содержащий все r_i. Вложение $R' \to R$ определяет гомоморфизм $f\colon H^1(R) \to H^1(R')$, ограничение которого дает гомоморфизм $\bar{f}\colon H^1(R)^F \to H^1(R')^F$. Если $\pi \in \mathrm{Ker}\, \bar{f}$, то π аннулирует R' и, следовательно, все r_i; в этом случае $\pi = 0$ по предположению. Отсюда следует, что $\mathrm{Ker}\, f$ не содержит ни одного ненулевого элемента, инвариантного относительно действия F. Следствие предложения 20 показывает тогда, что $\mathrm{Ker}\, f = 0$. В таком случае из предложения 23 следует, что гомоморфизм $R' \to R$ сюръективен, откуда $R' = R$, что и требовалось доказать.

Следствие. *Для того чтобы подгруппа* R *могла быть порождена* n *элементами (как нормальный делитель в* F*), необходимо и достаточно, чтобы выполнялось неравенство*

$$\dim H^1(R)^{F/R} \leqslant n.$$

Необходимость очевидна. Обратно, если $\dim H^1(R)^{F/R} \leqslant n$, то двойственность между группами $H^1(R)$ и R/R^* показывает, что существует набор из n элементов $r_i \in R$, для которых из равенств $\langle r_i, \pi \rangle = 0$ для всех i следует, что $\pi = 0$. Откуда получается искомый результат.

Замечание. Размерность группы $H^1(R)^{F/R}$ будем называть *рангом* нормального делителя R.

Применим предыдущее, как и раньше, к случаю, когда $F = F(n)$ — свободная про-p-группа, и положим $G = F/R$ (группа G задается, следовательно, „образующими и соотношениями").

Предложение 27. *Следующие два условия эквивалентны:*

(а) *Подгруппа R имеет конечный ранг r (как нормальный делитель в $F(n)$).*

(б) *Группа $H^2(G)$ имеет конечную размерность h_2. Если эти условия выполнены, то имеет место соотношение*

$$r = n - h_1 + h_2,$$

где h_1 обозначает ранг группы G (размерность $H^1(G)$).

Применим точную последовательность из п. 2.6 и примем во внимание, что $H^2(F(n)) = 0$. Получаем

$$0 \to H^1(G) \to H^1(F(n)) \to H^1(R)^G \xrightarrow{\delta} H^2(G) \to 0.$$

Из этой последовательности вытекает, что $H^1(R)^G$ и $H^2(G)$ одновременно конечны или бесконечны, откуда следует первая часть предложения. Вторая часть также получается из этой точной последовательности (составить альтернированную сумму размерностей).

Следствие. *Пусть G — такая про-р-группа, что $H^1(G)$ и $H^2(G)$ конечны. Пусть $x_1, \ldots, x_n$ — минимальная система образующих группы G. Тогда число соотношений r между образующими x_i равно размерности $H^2(G)$.*

[Элементы x_i определяют сюръективный морфизм $F(n) \to G$ с ядром R. „Число соотношений между x_i" есть по определению ранг подгруппы R (как нормального делителя в $F(n)$).]

Действительно, условие „система x_i является *минимальной* системой образующих" эквивалентно утверждению, что $n = \dim H^1(G)$; см. следствие предложения 25. В таком случае предыдущее предложение дает, что $r = h_2$. Следствие доказано.

Замечание. Доказательство предложения 27 существенно использует факт существования гомоморфизма δ: $H^1(R)^G \to H^2(G)$, определяемого из спектральной последовательности — гомоморфизма „трансгрессии". Можно

дать, однако, более элементарное его определение (см. Хохшильд — Серр [1]).

Будем исходить из расширения

$$1 \to R/R^* \to F/R^* \to G \to 1$$

с абелевым ядром R/R^*. Пусть π: $R/R^* \to \mathbf{Z}/p\mathbf{Z}$ — произвольный элемент из $H^1(R)^G$; он преобразует это расширение в некоторое расширение E_π группы G с помощью $\mathbf{Z}/p\mathbf{Z}$. Класс расширения E_π в $H^2(G)$ равен тогда $-\delta(\pi)$. В частности, в предположениях предыдущего следствия, мы получаем прямое определение изоморфизма δ: $H^1(R)^G \to H^2(G)$.

4.4. Теорема Шафаревича

Пусть G — конечная p-группа, $n(G)$ — минимальное число образующих группы G и $r(G)$ — минимальное число соотношений между этими образующими (в соответствующей свободной про-p-группе). Было показано, что $n(G) = \dim H^1(G)$ и $r(G) = \dim H^2(G)$.

[Можно было бы также ввести минимальное число $R(G)$ соотношений, определяющих G *как дискретную группу*. Очевидно, $R(G) \geqslant r(G)$, но я не вижу никаких доводов в пользу того, что всегда выполняется равенство.]

Предложение 28. *Для всякой конечной p-группы G имеет место неравенство $r(G) \geqslant n(G)$. Кроме того, разность $r(G) - n(G)$ равна рангу группы $H^3(G, \mathbf{Z})$.*

Точная последовательность $0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \to 0$ порождает точную последовательность когомологий

$$0 \to H^1(G) \to H^2(G, \mathbf{Z}) \xrightarrow{p} H^2(G, \mathbf{Z}) \to H^2(G) \to H^3(G, \mathbf{Z})_p \to 0,$$

где $H^3(G, \mathbf{Z})_p$ обозначает подгруппу группы $H^3(G, \mathbf{Z})$, порожденную элементами, аннулируемыми умножением на p. Так как группа G конечна, то все эти группы также конечны. Взяв альтернированное произведение их порядков, получаем 1. Это дает равенство

$$r(G) - n(G) = t,$$

где $t = \dim H^3(G, \mathbf{Z})_p$. Ясно, что t является также числом циклических слагаемых в группе $H^3(G, \mathbf{Z})$, т. е. рангом этой группы, откуда следует доказательство предложения.

Полученный выше результат приводит к постановке следующего вопроса: может ли быть малой разность $r(G)-n(G)$? Например, возможно ли, что $r(G)-n(G)=0$ для достаточно больших значений $n(G)$? [Во всех известных примерах $n(G)=0$, 1, 2 или 3, см. упражнение 2.] Была высказана более общая

Гипотеза (Шафаревич, Стокгольм, 1962). *Разность $r(G)-n(G)$ стремится к бесконечности с ростом $n(G)$.*

[Другими словами, для каждого целого k существует целое число N, такое, что как только $n(G)\geqslant N$, то $r(G)-n(G)\geqslant k$.]

Голод и Шафаревич ([1]) доказали следующий результат, из которого эта гипотеза вытекает:

Для любой конечной p-группы G

$$r(G)\geqslant\frac{1}{4}(n(G)-1)^2.$$

Отсюда следует

Теорема (Шафаревич). *Классическая проблема „башни полей классов" имеет отрицательное решение (т. е. существуют бесконечные „башни").*

Доказательство основано на следующем результате:

Предложение 29. *Пусть K/k — неразветвленное расширение Галуа числового поля k, группа Галуа которого является конечной p-группой. Предположим, что поле K не имеет никакого циклического неразветвленного расширения степени p. Обозначим через r_1 (соответственно r_2) число вещественных (соответственно комплексно сопряженных) вложений поля k в его алгебраическое замыкание $\bar{k}$. Тогда справедливо неравенство*

$$r(G)-n(G)\leqslant r_1+r_2.$$

Доказательство (см. Ивасава [3]). Положим

I_K — группа иделей поля K,

$C_K=I_K/K^*$ — группа классов иделей поля K,

U_K — подгруппа группы I_K, состоящая из элементов вида (x_v), где x_v — *единицы* поля K_v, для всех неархимедовых нормирований v,

$E_K = K^* \cap U_K$ — группа единиц поля K,
E_k — группа единиц поля k,
$Cl_K = I_K / U_K \cdot K^*$ — группа классов идеалов поля K.
Имеем точные последовательности

$$0 \to U_K/E_K \to C_K \to Cl_K \to 0,$$
$$0 \to E_K \to U_K \to U_K/E_K \to 0.$$

Согласно теории полей классов, тот факт, что K не имеет неразветвленных циклических расширений степени p, означает, что порядок группы Cl_K взаимно прост с p. Следовательно, группы когомологий $\hat{H}^q(G, Cl_K)$ тривиальны. То же самое верно и для групп когомологий $\hat{H}^q(G, U_K)$; это следует из неразветвленности расширения K/k. Таким образом, точная последовательность когомологий дает изоморфизмы

$$\hat{H}^q(G, C_K) \to \hat{H}^{q+1}(G, E_K).$$

С другой стороны, из теории полей классов известно, что группа $\hat{H}^q(G, C_K)$ изоморфна группе $\hat{H}^{q-2}(G, \mathbf{Z})$. Беря композицию этих изоморфизмов и полагая $q = -1$, получаем, что

$$\hat{H}^{-3}(G, \mathbf{Z}) = \hat{H}^0(G, E_K) = E_k/N(E_K).$$

Но группа $\hat{H}^{-3}(G, \mathbf{Z})$ двойственна группе $H^3(G, \mathbf{Z})$ (см. [M], стр. 305), следовательно, эти группы имеют одинаковый ранг. Применяя предложение 28, находим, что разность $r(G) - n(G)$ равна рангу группы $E_k/N(E_K)$. Далее по теореме Дирихле группа E_k порождается $r_1 + r_2$ элементами. Следовательно, ранг группы $E_k/N(E_K)$ не превосходит $r_1 + r_2$, что доказывает предложение. (Если поле k не содержит корней p-й степени из единицы, то разность $r(G) - n(G)$ можно ограничить даже числом $r_1 + r_2 - 1$.)

Возвратимся теперь к теореме. Пусть k — поле алгебраических чисел (чисто мнимое, если $p = 2$) и $k(p)$ — максимальное неразветвленное p-расширение Галуа поля k. Его группа Галуа G_k является, следовательно, про-p-группой. Нам надо доказать (используя теорему Голода — Шафаревича), что существует такое поле k, для которого

$k(p)$ является бесконечным расширением. Предположим, что расширение $k(p)/k$ конечно. Применяя тогда к нему предыдущее предложение, получаем неравенство

$$r(G_k) - n(G_k) \leqslant r_1 + r_2 \leqslant [k : \mathbf{Q}].$$

Но теория полей классов позволяет вычислить $n(G_k)$. Это число совпадает с рангом p-примарной компоненты группы Cl_k. Можно построить поля k ограниченной степени, для которых $n(G_k) \to \infty$. Отсюда получаем противоречие с теоремой Голода — Шафаревича, что и требовалось доказать.

Пример. Возьмем $p = 2$. Пусть $p_1, \ldots, p_N$ — попарно различные простые числа, сравнимые с 1 по mod 4. Пусть $k = \mathbf{Q}(\sqrt{-p_1 \ldots p_N})$. Поле k является чисто мнимым квадратичным расширением $\mathbf{Q}$. Следовательно, для него $r_1 = 0$, $r_2 = 1$. С другой стороны, легко видеть, что его квадратичные расширения, порожденные $\sqrt{p_i}$, $1 \leqslant i \leqslant N$, все неразветвлены и независимы. Следовательно, $n(G_k) \geqslant N$ и $r(G_k) - n(G_k) \leqslant 1$.

Поэтому для получения бесконечной „башни“ достаточно положить $k = \mathbf{Q}(\sqrt{3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$.

Упражнения. 1) Доказать неравенство $r(G) \geqslant n(G)$ предложения 28, переходя к факторгруппе по коммутанту.

2) Пусть n — целое число. Рассмотрим системы $c(i, j, k)$ целых чисел с i, j, k из интервала $[1, n]$, альтернированные по (i, j).

(а) Показать, что для всякого $n \geqslant 3$ существует по крайней мере одна такая система, обладающая следующим свойством:

(*) Если элементы $x_1, \ldots, x_n$ некоторой алгебры Ли $\mathfrak{g}$ характеристики p удовлетворяют соотношениям

$$[x_i, x_j] = \sum_k c(i, j, k)\, x_k,$$

то $x_i = 0$ для всех i.

(б) Каждой системе $c(i, j, k)$ сопоставим про-p-группу G_c, определенную n образующими x_i и соотношениями

$$(x_i, x_j) = \prod x_k^{p \cdot c(i, j, k)}, \quad i < j,$$

где $(x, y) = xyx^{-1}y^{-1}$.

Показать, что $\dim H^1(G_c) = n$ и $\dim H^2(G_c) = \frac{n(n-1)}{2}$.

(в) Предположим, что $p \neq 2$. Показать, что если система $c(i, j, k)$ удовлетворяет условию (*) упражнения (а), то соответствующая группа конечна.

[Построить фильтрацию группы G, полагая $G_1 = G$, $G_{n+1} = G_n^p \cdot (G, G_n)$. Соответствующий градуированный объект $\operatorname{gr}(G)$ является алгеброй Ли над кольцом $\mathbf{Z}/p\mathbf{Z}[\pi]$, где $\deg \pi = 1$. Показать, что в алгебре $\operatorname{gr}(G)$ закон умножения имеет вид

$$[x_i, x_j] = \sum c(i, j, k)\, \pi x_k.$$

Вывести отсюда, что $\operatorname{gr}(G)\left[\frac{1}{\pi}\right] = 0$, откуда вытекают конечность $\operatorname{gr}(G)$ и, следовательно, конечность группы G.]

(г) Что надо изменить в предыдущем, если $p = 2$?

(д) Показать, что про-p-группа, порожденная тремя образующими x, y, z и тремя соотношениями

$$xyx^{-1} = y^{1+p}, \quad yzy^{-1} = z^{1+p}, \quad zxz^{-1} = x^{1+p},$$

конечна (см. Меннике [1]).

4.5. Группы Пуанкаре

Пусть $n \geqslant 1$ — целое число и G — некоторая про-p-группа. Мы говорим, что G является *группой Пуанкаре размерности* n, если она удовлетворяет следующим условиям:

(i) *группы* $H^i(G) = H^i(G, \mathbf{Z}/p\mathbf{Z})$ *конечны для всех* i;

(ii) $\dim H^n(G) = 1$;

(iii) $\cup$-*произведение*

$$H^i(G) \times H^{n-i}(G) \to H^n(G)$$

является билинейной невырожденной формой для любого $i \geqslant 0$.

Эти условия можно выразить короче, сказав, что алгебра когомологий $H^*(G)$ конечномерна и удовлетворяет двойственности Пуанкаре. Отметим, что условие (iii) влечет равенства $H^i(G) = 0$ для всех $i > n$. Следовательно, $\operatorname{cd}(G) \leqslant n$.

Примеры. (1) Группа $\mathbf{Z}_p$ является единственной группой Пуанкаре размерности 1 (с точностью до изоморфизма).

(2) Если G — группа Пуанкаре размерности 2, то $\dim H^2(G) = 1$, т. е. G может быть определена одним соотношением (см. п. 4.3); это соотношение, однако, не произвольно. Оно может быть задано в некотором каноническом виде ($p \neq 2$); см. доклад 252 на семинаре Бурбаки о работах Дёмушкина.

[Строение групп Дёмушкина в исключительном случае $p=2$ было изучено Дёмушкиным [2*] и Ж. Лабютом [1*].]

(3) Лазар показал, что всякая достаточно малая открытая подгруппа компактной аналитической группы X над $\mathbf{Q}_p$ размерности n является группой Пуанкаре размерности n. Это дает большой запас таких групп (столько, и даже больше, сколько существует алгебр Ли размерности n над $\mathbf{Q}_p$).

Пусть G — группа Пуанкаре размерности n. Тогда из условия (i) и из следствия предложения 20 вытекает, что группы $H^i(G, A)$ будут конечными для любого конечного G-модуля A. Так как, с другой стороны, $\mathrm{cd}(G) = n$, то для G определен *дуализирующий* модуль I (см. п. 3.5). Мы сейчас увидим, что он доставляет настоящую „двойственность Пуанкаре“.

Предложение 30. *Пусть G является про-p-группой Пуанкаре размерности n и I — ее дуализирующий модуль. Тогда:*

(а) *модуль I изоморфен $\mathbf{Q}_p/\mathbf{Z}_p$ (как абелева группа),*

(б) *канонический гомоморфизм i: $H^n(G, I) \to \mathbf{Q}/\mathbf{Z}$ является изоморфизмом на группу $\mathbf{Q}_p/\mathbf{Z}_p$ (отождествленную с подгруппой группы $\mathbf{Q}/\mathbf{Z}$),*

(в) *для каждого модуля $A \in \mathscr{C}_G^f$ и каждого целого числа i $\cup$-произведение*

$$H^i(G, A) \times H^{n-i}(G, \tilde{A}) \to H^n(G, I) = \mathbf{Q}_p/\mathbf{Z}_p$$

осуществляет двойственность между двумя конечными группами

$$H^i(G, A) \quad и \quad H^{n-i}(G, \tilde{A}).$$

[Здесь $\mathscr{C}_G^f$ обозначает категорию конечных p-примарных дискретных G-модулей и $\tilde{A} = \mathrm{Hom}(A, I)$ для каждого G-модуля A, см. п. 3.5.]

Доказательство проводится в несколько этапов.

(1) *Двойственность имеет место, когда модуль A аннулируется умножением на p.*

В этом случае A является векторным $\mathbf{Z}/p\mathbf{Z}$-пространством. Двойственное к нему пространство мы будем обозначать через A^* (позднее будет установлено, что оно отождествляется с $\tilde{A}$). Для каждого целого i $\cup$-произведение

$$H^i(G, A) \times H^{n-i}(G, A^*) \to H^n(G) = \mathbf{Z}/p\mathbf{Z}$$

определяет некоторую билинейную форму. Эта форма невырождена. Действительно, по самому определению группы Пуанкаре это верно в случае, когда $A = \mathbf{Z}/p\mathbf{Z}$. В силу следствия предложения 20 достаточно показать, что если доказываемое утверждение верно для членов B и C точной последовательности $0 \to B \to A \to C \to 0$, то оно верно также и для A. Но это следует из небольшой диаграммы стандартного типа. Точнее, определение выписанной выше билинейной формы эквивалентно заданию гомоморфизма

$$\alpha_i\colon H^i(G, A) \to H^{n-i}(G, A^*)^*,$$

и утверждение о ее невырожденности означает, что α_i является изоморфизмом. С другой стороны, имеем точную последовательность

$$0 \to C^* \to A^* \to B^* \to 0,$$

откуда, переходя к когомологиям и дуализируя, получаем диаграмму

$$\begin{array}{ccccccccc}
\ldots \to & H^{i-1}(G, C) & \to & H^i(G, B) & \to & H^i(G, A) & \to & H^i(G, C) & \to \ldots \\
& \downarrow & - & \downarrow & + & \downarrow & + & \downarrow & \\
\ldots \to & H^{j+1}(G, C^*)^* & \to & H^j(G, B^*)^* & \to & H^j(G, A^*)^* & \to & H^j(G, C^*)^* & \to \ldots,
\end{array}$$

где $j = n - i$.

Простым подсчетом на коцепях проверяется, что квадраты этой диаграммы коммутативны с точностью

до знака [вернее, квадраты, отмеченные знаком $+$, коммутативны, а квадрат со знаком $-$ становится коммутативным при умножении на $(-1)^i$]. Поскольку вертикальные стрелки, исходящие из $H^i(G, B)$ и $H^i(G, C)$, обозначают отображения, являющиеся изоморфизмами, то таким же будет и отображение, обозначенное стрелкой, исходящей из $H^i(G, A)$, что доказывает наше утверждение.

(2) *Подгруппа* I_p *в* I, *порожденная элементами, аннулируемыми умножением на* p, *изоморфна* $\mathbf{Z}/p\mathbf{Z}$.

Возьмем в качестве A группу, аннулируемую умножением на p. Тогда в силу доказанного выше результата группа $H^n(G, A)^*$ функториально изоморфна группе $\mathrm{Hom}_G(A, \mathbf{Z}/p\mathbf{Z})$. С другой стороны, из определения дуализирующего модуля следует, что эта группа изоморфна также группе $\mathrm{Hom}_G(A, I_p)$. Единственность представляющего объекта для данного функтора обеспечивает изоморфизм $I_p = \mathbf{Z}/p\mathbf{Z}$.

(3) *Дуализирующий модуль* I *изоморфен* (*как абелева группа*) *либо* $\mathbf{Z}/p^k\mathbf{Z}$, *либо* $\mathbf{Q}_p/\mathbf{Z}_p$.

Это следует из соотношения $I_p = \mathbf{Z}/p\mathbf{Z}$ и из элементарных свойств p-примарных периодических групп.

(4) *Всякая открытая подгруппа* U *группы* G *является группой Пуанкаре размерности* n, *и гомоморфизм* $\mathrm{Cor}\colon H^n(U) \to H^n(G)$ *является изоморфизмом.*

Пусть $A = M_G^U(\mathbf{Z}/p\mathbf{Z})$. Легко проверить, что модуль A^* изоморфен модулю A, и двойственность, установленная в (1), показывает, что группы $H^i(U)$ и $H^{n-i}(U)$ двойственны друг другу. В частности, $\dim H^n(U) = 1$. Отсюда, поскольку гомоморфизм $\mathrm{Cor}\colon H^n(U) \to H^n(G)$ сюръективен (см. п. 3.3, лемма 4), следует, что он является изоморфизмом. Наконец, нетрудно показать, что двойственность, существующая между $H^i(U)$ и $H^{n-i}(U)$, является не чем иным, как двойственностью, определенной $\cup$-произведением.

(5) *Для любого* $A \in \mathscr{C}_G^f$ *положим* $T^i(A) = \varprojlim H^i(U, A)$, *где* U *пробегает все открытые подгруппы в* G (*а гомоморфизмы — соответствующие коограничения*). *Тогда* $T^i(A) = 0$ *для всех* $i \neq n$ *и* $T^n(A)$ — *точный функтор*

относительно A (со значениями в категории проконечных абелевых групп).

Ясно, что T^i составляют когомологический функтор (функтор $\varprojlim$ точен на категории проконечных групп). Для доказательства того, что $T^i = 0$ при $i \neq n$, достаточно, следовательно, проверить это в случае, когда $A = \mathbf{Z}/p\mathbf{Z}$. Но тогда группы $H^i(U)$ двойственны группам $H^{n-i}(U)$ и все сводится к доказательству того, что $\varinjlim H^j(U) = 0$ для $j \neq 0$. Этот факт тривиален, если учесть, что предел берется по системе гомоморфизмов-ограничений (он верен для любой проконечной группы и для любого модуля). Точность функтора T^n автоматически следует из равенства нулю всех T^i, $i \neq n$.

(6) *Модуль I (как абелева группа) изоморфен модулю $\mathbf{Q}_p/\mathbf{Z}_p$.*

Мы знаем, что группа $H^n(U, A)$ двойственна группе $\mathrm{Hom}_U(A, I)$. Переходя к пределу, получаем, что группа $T^n(A) = \varprojlim H^n(U, A)$ двойственна группе $\varinjlim \mathrm{Hom}_U(A, I) = \mathrm{Hom}(A, I)$. В силу утверждения (5) функтор $\mathrm{Hom}(A, I)$ точен; это означает, что группа I является $\mathbf{Z}$-делимой, и сопоставление с (3) показывает, что она изоморфна группе $\mathbf{Q}_p/\mathbf{Z}_p$.

(7) *Гомоморфизм $H^n(G, I) \to \mathbf{Q}_p/\mathbf{Z}_p$ является изоморфизмом.*

Группа всех $\mathbf{Z}$-эндоморфизмов группы I изоморфна группе $\mathbf{Z}_p$ (действующей очевидным образом на I). Так как это действие коммутирует с действием G, то мы получаем, что $\mathrm{Hom}_G(I, I) = \mathbf{Z}_p$. Но, с другой стороны, группа $\mathrm{Hom}_G(I, I)$ двойственна группе $H^n(G, I)$, см. п. 3.5. Имеем, следовательно, канонический изоморфизм $H^n(G, I) \to \mathbf{Q}_p/\mathbf{Z}_p$, и легко показать, что этот изоморфизм индуцирован гомоморфизмом i.

(8) *Окончание доказательства.*

Осталось доказать пункт (в), иначе говоря, двойственность между $H^i(G, A)$ и $H^{n-i}(G, \tilde{A})$. Эта двойственность справедлива для $A = \mathbf{Z}/p\mathbf{Z}$ по предположению. Исходя из этого, применим процесс „отвинчивания“ точно так же,

как это делалось в пункте (1). Достаточно только заметить, что если $0 \to A \to B \to C \to 0$ — точная последовательность в $\mathscr{C}_G^f$, то последовательность $0 \to \widetilde{C} \to \widetilde{B} \to \widetilde{A} \to 0$ будет также точной (это следует из того, что группа I делима) и можно тогда использовать диаграмму, аналогичную той, которая рассматривалась в утверждении (1).

Следствие. *Всякая открытая подгруппа группы Пуанкаре является также группой Пуанкаре той же размерности.*

Это было установлено в процессе доказательства предложения.

Замечания. 1. Тот факт, что группа I изоморфна группе $\mathbf{Q}_p/\mathbf{Z}_p$, означает, что $\widetilde{\widetilde{A}}$ *канонически изоморфен* A (как G-модуль). Мы имеем, таким образом, превосходную двойственность.

2. Обозначим через U_p группу p-адических единиц (т. е. обратимых элементов из кольца $\mathbf{Z}_p$). Группа U_p изоморфна группе автоморфизмов группы I. Поскольку G действует на I, то это действие задает некоторый *канонический гомоморфизм*

$$\chi\colon G \to U_p.$$

Гомоморфизм χ непрерывен и однозначно (с точностью до изоморфизма) определяет G-модуль I. Можно сказать, что он играет ту же роль, что и гомоморфизм ориентации $\pi_1 \to \{\pm 1\}$ в топологии. Отметим, что, поскольку G является про-p-группой, гомоморфизм χ принимает значения в подгруппе $U_p^{(1)}$ группы U_p, состоящей из элементов, сравнимых с 1 по модулю p. Гомоморфизм χ относится к числу наиболее интересных инвариантов группы G; мы сейчас увидим, что он определяет, в частности, строгую когомологическую размерность группы G.

Предложение 31. *Пусть G — про-p-группа Пуанкаре размерности n и $\chi\colon G \to U_p$ — ассоциированный с ней гомоморфизм. Для того чтобы* $\operatorname{scd}(G)$ *была равна $n+1$, необходимо и достаточно, чтобы образ χ был конечен.*

Утверждение о конечности $\operatorname{Im} \chi$ равносильно следующему: существует такая открытая подгруппа U в G, что $\chi(U) = \{1\}$. Последнее условие означает, что группа I^U содержит группу $\mathbf{Q}_p/\mathbf{Z}_p$ (и в действительности совпадает с ней). В силу предложения 19 отсюда следует требуемое.

Замечание. Структура группы $U_p^{(1)}$ хорошо известна: при $p \neq 2$ эта группа изоморфна $\mathbf{Z}_p$, а при $p = 2$ — произведению $\{\pm 1\} \times \mathbf{Z}_2$ (см., например, [CL], стр. 220). Предложение 31 можно, следовательно, переформулировать в виде: при $p \neq 2$ равенство $\operatorname{scd}(G) = n + 1$ эквивалентно утверждению, что гомоморфизм χ тривиален; при $p = 2$ оно эквивалентно тому, что $\chi(G)$ равно 1 или $\{\pm 1\}$.

Следующее предложение используется при изучении „групп Дёмушкина“.

Предложение 32. *Пусть G — про-p-группа и n — целое число, большее или равное* 1. *Предположим, что группы $H^i(G)$ конечны для всех $i \leqslant n$,* $\dim H^n(G) = 1$ *и $\cup$-произведение $H^i(G) \times H^{n-i}(G) \to H^n(G)$ невырождено для всех $i \leqslant n$. Если, кроме того, группа G бесконечна, то она является группой Пуанкаре размерности n.*

Достаточно, очевидно, доказать, что $H^{n+1}(G) = 0$. Для этого нужно установить прежде всего некоторые свойства двойственности.

(1) *Двойственность для конечных G-модулей A, аннулируемых умножением на p.*

Поступаем точно так же, как и в пункте (1) доказательства предложения 30. При помощи $\cup$-произведения определяем гомоморфизмы

$$\alpha_i\colon H^i(G, A) \to H^{n-i}(G, A^*)^*, \quad 0 \leqslant i \leqslant n.$$

По предположению они являются изоморфизмами в случае, когда $A = \mathbf{Z}/p\mathbf{Z}$. С помощью метода „отвинчивания“ легко показывается, что эти гомоморфизмы являются изоморфизмами для всех $1 \leqslant i \leqslant n-1$ и любого модуля A и что α_0 сюръективен, а α_n инъективен. [Различие с ситуацией предложения 30 пропадает, если группы H^{n+1} равны нулю. Они доставляют неприятности в концах точных последовательностей.]

(2) *Функтор* $H^0(G, A)$ *является костирающим*[1]).

Это общее свойство всех проконечных групп, порядок которых делится на p^∞.

Пусть A аннулируется умножением на p^k (число k здесь уже не обязательно равно 1). Выберем открытую подгруппу U в G, тривиально действующую на A, а затем открытую подгруппу V в U, индекс которой делится на p^k. Положим $A' = M_G^V(A)$ и рассмотрим сюръективный гомоморфизм π: $A' \to A$, определенный в п. 2.5. При переходе к H^0 получаем

$$\mathrm{Cor}: H^0(V, A) \to H^0(G, A).$$

Гомоморфизм Cor является здесь нулевым. Действительно, он совпадает с гомоморфизмом взятия нормы $N_{G/V}$, который в свою очередь равен $(U: V) N_{G/U}$. Следовательно, нулевым является и гомоморфизм $H^0(G, A') \to H^0(G, A)$, а это доказывает тот факт, что функтор H^0 — костирающий.

3) *Двойственность в размерностях* 0 *и* n.

Речь идет о доказательстве того, что α_0 и α_n биективны для всякого модуля A, аннулируемого умножением на p. Достаточно (благодаря транспонированию) проделать это для α_0. Рассмотрим точную последовательность

$$0 \to B \to C \to A \to 0,$$

такую, что гомоморфизм $H^0(G, C) \to H^0(G, A)$ является нулевым. Имеем тогда следующую диаграмму:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(G, A) & \longrightarrow & H^1(G, B) & \longrightarrow & H^1(G, C) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^n(G, C^*)^* & \to & H^n(G, A^*)^* & \to & H^{n-1}(G, B^*)^* & \to & H^{n-1}(G, C^*)^*. \end{array}$$

Стрелки, относящиеся к H^1, обозначают отображения, являющиеся изоморфизмами; значит, гомоморфизм α_0 инъективен, отсюда следует требуемое, поскольку мы уже знаем, что α_0 всегда сюръективен.

(4) *Функтор* H^n *точен справа.*

---

[1]) Понятие костирающего функтора является двойственным к понятию стирающего функтора, см. примечание на стр. 19. — *Прим. перев.*

Это выводится с помощью двойственности из того, что функтор H^0 является точным слева.

(5) *Окончание доказательства.*

Из предыдущих результатов следует, что $\mathrm{cd}(G) \leqslant n$. В самом деле, если $x \in H^{n+1}(G, A)$, то он индуцирует 0 на некоторой открытой подгруппе U группы G и задает, следовательно, нуль в группе $H^{n+1}(G, M_G^U(A))$. Пользуясь точной последовательностью и тем фактом, что функтор H^n точен справа, получаем, что $x = 0$. Предложение доказано.

Упражнения. 1) Построить примеры конечных p-групп, когомологии которых удовлетворяют двойственности Пуанкаре до некоторой размерности.

2) Пусть G — фундаментальная группа некоторой компактной поверхности S рода g. Предположим, что $g \geqslant 1$, если S ориентируема, и $g \geqslant 2$ в противном случае. Через $\hat{G}_p$ обозначим p-пополнение группы G. Показать, что G_p является группой Пуанкаре размерности 2 и что для каждого конечного p-примарного $\hat{G}_p$-модуля A гомоморфизм

$$H^i(\hat{G}_p, A) \to H^i(G, A)$$

является изоморфизмом. Показать, что строгая когомологическая размерность группы $\hat{G}_p$ равна 3, и объяснить смысл инварианта χ.

3) Пусть G — про-p-группа, порожденная двумя образующими x, y, связанными единственным соотношением

$$xyx^{-1} = y^q, \quad q \in \mathbf{Z}_p, \quad q \equiv 1 \bmod p.$$

Показать, что G является группой Пуанкаре размерности 2 и ее инвариант χ задается формулами

$$\chi(y) = 1, \quad \chi(x) = q.$$

В каком случае строгая когомологическая размерность этой группы равна 3? Применить это к силовской p-подгруппе аффинной группы $ax + b$ над $\mathbf{Z}_p$.

4) Пусть G — некоторая про-p-группа Пуанкаре размерности n и I — ее дуализирующий модуль. Положим $J = \mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, I)$. Тогда G-модуль J изоморфен $\mathbf{Z}_p$ как

компактная группа и G действует на нем посредством гомоморфизма χ.

(а) Пусть A — некоторый конечный p-примарный G-модуль. Положим $A_0 = A \otimes J$ (тензорное произведение берется над $\mathbf{Z}_p$). Показать, что модуль A_0 канонически изоморфен модулю A^*, двойственному к A.

(б) Для каждого целого $i \geqslant 0$ рассмотрим проективный предел $H_i(G, A)$ групп *гомологий* $H_i(G/U, A)$, где U—всевозможные открытые нормальные делители в G, тривиально действующие на A. Установить некоторый канонический изоморфизм

$$H_i(G, A) = H^{n-1}(G, A_0).$$

[Использовать существующую двойственность между $H_i(G/U, A)$ и $H^i(G/U, A^*)$, см. [M], стр. 303—304.]

§ 5. НЕАБЕЛЕВЫ КОГОМОЛОГИИ

На всем протяжении этого параграфа G обозначает проконечную группу.

5.1. Определение H^0 и H^1

Условимся называть *G-множеством* дискретное топологическое пространство E, на котором непрерывно действует группа G; так же как и в случае G-модулей, это равносильно утверждению, что $E = \bigcup E^U$, где U пробегает множество всех открытых подгрупп в G (через E^U обозначено подмножество элементов из E, инвариантных относительно U). Для любых $s \in G$ и $x \in E$ образ $s(x)$ элемента x при действии s будет обозначаться через ${}^s x$ [а не x^s, дабы избежать ужасной формулы $x^{(st)} = (x^t)^s$]. Пусть E и E' — два G-множества. *Морфизмом* E в E' будем называть любое отображение $f\colon E \to E'$, коммутирующее с действием G; если желательно указать на группу G, будем называть такое отображение „G-морфизмом“. G-множества образуют категорию.

Всякую группу A в этой категории мы называем *G-группой*. Иначе говоря, это некоторое G-множество, снабженное G-инвариантной структурой группы (т. е. ${}^s(xy) = {}^s x {}^s y$). В случае когда A коммутативна, получается обычное понятие *G-модуля*, использовавшееся в предыдущих параграфах.

Пусть E — некоторое G-множество и $H^0(G, E) = E^G$ (множество элементов из E, инвариантных относительно G). Если E является G-группой, то $H^0(G, E)$ — группа.

Пусть A — произвольная G-группа. Назовем *одномерным коциклом со значениями* в A непрерывное отображение $s \to a_s$ группы G в A, удовлетворяющее условию

$$a_{st} = a_s {}^s a_t, \qquad (s, t \in G).$$

Множество всех таких коциклов будем обозначать через $Z^1(G, A)$. Два коцикла a и a' называются *когомологичными*, если существует элемент $b \in A$, такой, что $a'_s = b^{-1} a_s {}^s b$. Это некоторое отношение эквивалентности на множестве $Z^1(G, A)$. Фактормножество по этому отношению эквивалентности обозначим через $H^1(G, A)$. Оно называется одномерным множеством когомологий группы G с коэффициентами в A, и оно обладает отмеченным элементом (называемым „нейтральным элементом“, хотя в общем случае на $H^1(G, A)$ нет никакого закона композиции) — классом единичного коцикла, — который обозначается через 0 или 1 (безразлично). Немедленно проверяется, что

$$H^1(G, A) = \varinjlim H^1(G/U, A^U),$$

где U пробегает множество всех открытых нормальных делителей в G.

Множества когомологий $H^0(G, A)$ и $H^1(G, A)$ функториально зависят от группы A и в случае, когда она коммутативна, совпадают с группами когомологий в размерностях 0 и 1 соответственно.

Замечания. 1. Хотелось бы определить также $H^2(G, A)$, $H^3(G, A)$, ... Есть люди (Дедекер, например), утверждающие, что они знают хорошее определение $H^2(G, A)$; автор долгое время был настроен скептически, но теперь начинает верить, что они правы.

2. Неабелевы когомологии H^1 являются пунктированными множествами; имеет смысл, следовательно, понятие точной последовательности (прообраз нейтрального элемента равен образу предыдущего отображения). Однако такая точная последовательность не дает никаких сведений об отношении эквивалентности, определяемом каким-то

из ее отображений. Мы устраним этот недостаток (особенно ощутимый в [CL], стр. 131—134), введя понятие „скручивания“, которому будет посвящен п. 5.3.

5.2. Главные однородные пространства над A, новое определение $H^1(G, A)$

Пусть A — некоторая G-группа и E — какое-либо G-множество. Будем говорить, что A *действует слева* на E (перестановочно с действием G), если она действует на E в обычном смысле и ${}^s(a \cdot x) = {}^s a \cdot {}^s x$ для всех $a \in A$ и $x \in E$ (иначе говоря, каноническое отображение $A \times E$ в E является G-морфизмом). Мы применяем для этого обозначение ${}_A E$, подчеркивая тем самым, что A действует слева (аналогично обозначается действие справа).

Главным однородным пространством над A называется непустое G-множество P, на котором A действует справа (перестановочно с действием G) так, что P становится „аффинным пространством“ над A (т. е. для любой пары x, $y \in P$, существует единственный элемент $a \in A$, такой, что $y = x \cdot a$). Очевидным образом определяется понятие изоморфизма двух таких пространств.

Предложение 33. *Пусть A — произвольная G-группа. Тогда существует биективное соответствие между множеством классов изоморфных главных однородных пространств над A и множеством $H^1(G, A)$.*

Пусть $P(A)$ обозначает первое из этих множеств. Определим отображение

$$\lambda\colon P(A) \to H^1(G, A)$$

следующим способом. Пусть $P \in P(A)$. Выберем некоторую точку $x \in P$. Если $s \in G$, то ${}^s x$ также принадлежит P и, следовательно, существует элемент $a_s \in A$, такой, что ${}^s x = x \cdot a_s$. Легко проверить, что a_s — коцикл. При замене x на $x \cdot b$ коцикл a_s заменяется на когомологичный ему коцикл $b^{-1} a_s {}^s b$. Класс коцикла a_s условимся считать образом $\lambda(P)$ элемента $P \in P(A)$.

Определим обратное отображение $\mu\colon H^1(G, A) \to P(A)$. Пусть $a_s \in Z^1(G, A)$. Обозначим через P_a группу A, на которой G действует согласно следующей „скрученной“ формуле

$${}^{s'} x = a_s \cdot {}^s x.$$

Группа A действует на P_a с помощью сдвигов, превращая его, таким образом, в некоторое главное однородное пространство. Когомологичные коциклы приводят при такой конструкции к изоморфным пространствам. Это позволяет определить отображение μ. Нетрудно проверить, что $\lambda \circ \mu = 1$ и $\mu \circ \lambda = 1$.

Замечание. Главные однородные пространства, рассмотренные выше, являлись *правыми* главными однородными пространствами. Аналогично определяются *левые* главные однородные пространства. Мы оставляем читателю определить связь между этими двумя понятиями.

5.3. Скручивание

Пусть A — некоторая G-группа и P — главное однородное пространство над A. Пусть далее F — какое-либо G-множество, на котором A действует слева (перестановочно с действием G). На множестве $P \times F$ рассмотрим отношение эквивалентности, которое отождествляет всякий элемент (p, f) с элементом $(p \cdot a, a^{-1}f)$, $a \in A$. Это отношение совместимо с действием G, и, таким образом, фактормножество по нему снабжено структурой G-множества. Мы будем обозначать его через $P \times^A F$ или через ${}_pF$. Каждый элемент из $P \times^A F$ записывается в виде $p \cdot f$ и удовлетворяет тождествам $(p \cdot a) f = p(af)$, $a \in A$, что оправдывает обозначение. Заметим, что для всякого элемента $p \in P$ отображение $f \to p \cdot f$ является биекцией множества F на множество ${}_pF$; в этом смысле говорят, что ${}_pF$ получается из F *„скручиванием“ с помощью* P.

Операцию скручивания можно определить также и с точки зрения коциклов. Пусть $(a_s) \in Z^1(G, A)$ — одномерный коцикл. Обозначим через ${}_aF$ множество F, на котором G действует по формуле

$$^{s'}f = a_s \cdot {}^s f.$$

В этом случае мы говорим, что ${}_aF$ получается из F *скручиванием с помощью коцикла* a_s.

Легко установить связь между этими двумя точками зрения: пусть $p \in P$, тогда элемент p определяет некоторый коцикл a_s посредством формулы ${}^sp = p \cdot a_s$. Отображение $f \to p \cdot f$ определяет *изоморфизм* G-*множе-*

ства ${}_aF$ *на G-множество* ${}_pF$. В самом деле,

$$p \cdot {}^{s'}f = p \cdot a_s \cdot {}^sf = {}^sp \cdot {}^sf = {}^s(p \cdot f).$$

Это показывает, в частности, что если a и b когомологичны, то множество ${}_aF$ изоморфно ${}_bF$.

Замечание. Надо отметить, что, вообще говоря, не существует канонического изоморфизма между множествами ${}_aF$ и ${}_bF$ и, следовательно, эти множества *нельзя отождествить*, как это ни соблазнительно было бы сделать. В частности, ***не имеет смысла*** обозначение ${}_\alpha F$, $\alpha \in H^1(G, A)$. Излишне говорить, что аналогичные трудности существуют также и в топологии – в теории расслоенных пространств (которой мы сейчас следуем). Операция скручивания обладает рядом элементарных свойств:

(а) ${}_aF$ функториально по F (относительно A-морфизмов $F \to F'$).

(б) Имеет место соотношение ${}_a(F \times F') = {}_aF \times {}_aF'$.

(в) Если некоторая G-группа B действует справа на F (коммутируя с действием A), то B также действует и на ${}_aF$.

(г) Если F снабжено A-инвариантной структурой G-группы, то ${}_aF$ также имеет структуру G-группы.

Примеры. (1) Возьмем в качестве F саму группу A, а действие определим как левые сдвиги. Так как правые сдвиги коммутируют с левыми, то сформулированное выше свойство (в) показывает, что A действует справа на ${}_aF$. Таким образом, мы получаем некоторое главное однородное пространство над A (которое в предыдущем пункте обозначалось через ${}_aP$). В обозначениях, принятых выше, это записывается в виде

$$P \times {}^AA = P,$$

формула упрощения, которую можно сопоставить с формулой $E \underset{A}{\otimes} A = E$.

(2) В качестве F возьмем снова группу A, действующую на себе *внутренними автоморфизмами*. Поскольку это действие согласовано со структурой группы A, то свойство (г) показывает, что ${}_aA$ ***является G-группой*** [можно скрутить также всякий нормальный делитель в A]. По определению ${}_aA$ как множество совпадает с A, а

действие G на ${}_aA$ задается формулой

$$^{s\prime}x = a_s \cdot {}^s x \cdot a_s^{-1} \qquad (s \in G,\ x \in A).$$

Предложение 34. *Пусть F — такое G-множество, на котором A действует слева (перестановочно с действием G); пусть a — коцикл группы G со значениями в A. Тогда действие скрученной группы ${}_aA$ на ${}_aF$ перестановочно с действием G.*

Нужно показать, что отображение $(a, x) \to ax$ множества ${}_aA \times {}_aF$ в ${}_aF$ является G-морфизмом, что проверяется непосредственным вычислением.

Следствие. *Если P — главное однородное пространство над A, то группа ${}_PA$ действует слева на P и превращает P в левое главное однородное пространство над ${}_PA$.*

Тот факт, что ${}_PA$ действует на P, есть частный случай предложения 34 (или устанавливается непосредственно). Очевидно, что на P задается, таким образом, структура левого главного однородного пространства над ${}_PA$.

Замечание. Пусть A и A' — две G-группы. Очевидным способом определяется понятие (A, A')-главного однородного пространства: это левое главное однородное пространство над A и правое главное однородное пространство над A', причем действия A и A' коммутируют. Пусть P — такое пространство, тогда предыдущее следствие показывает, что A отождествляется с ${}_PA'$. Если Q есть (A', A'')-главное однородное пространство (A'' — некоторая другая G-группа), то пространство $P \circ Q = P \times^{A'} Q$ снабжается канонической структурой (A, A'')-главного однородного пространства. Мы получаем, таким образом, некоторый закон композиции (не всюду определенный), на множестве „дважды главных однородных пространств".

Предложение 35. *Пусть P — правое главное однородное пространство над G-группой A и $A' = {}_PA$ — соответствующая группа. Если каждому правому главному однородному пространству Q над A' сопоставить композицию $Q \circ P$, то получится биективное соответствие между множествами $H^1(G, A')$ и $H^1(G, A)$, которое отображает нейтральный элемент из $H^1(G, A')$ в класс π множества $H^1(G, A)$, соответствующий пространству P.*

[Более кратко, если скрутить A с помощью некоторого коцикла со значениями в A, то получится группа A', имеющая то же множество одномерных когомологий, что и A.]

Определим противоположное к P пространство $\overline{P}$ следующим образом: $\overline{P}$ — это (A, A')-главное однородное пространство, тождественное P как G-множество, на котором группа A действует слева по формуле $a \cdot p = p \cdot a^{-1}$, а группа A' — справа по формуле $p \cdot a' = a'^{-1} \cdot p$. Сопоставляя каждому правому главному однородному пространству R над A композицию $R \circ \overline{P}$, получаем, что на классах это сопоставление является обратным к заданному отображению $Q \longrightarrow Q \circ P$, что доказывает предложение 35.

Предложение 35′. *Пусть $a \in Z^1(G, A)$ — некоторый коцикл и $A' = {}_aA$. Если каждому коциклу a'_s со значениями в A' сопоставить произведение $a'_s \cdot a_s$, то получится коцикл со значениями в A и это сопоставление является биекцией*

$$t_a\colon Z^1(G, A') \to Z^1(G, A).$$

При переходе к когомологиям t_a определяет также некоторую биекцию

$$\tau_a\colon H^1(G, A') \to H^1(G, A),$$

которая отображает нейтральный элемент из $H^1(G, A')$ в класс α элемента a.

В сущности это некоторая переформулировка предыдущего предложения в терминах коциклов. Это предложение можно было бы доказать также и непосредственным вычислением.

Замечания. 1. В случае когда группа A абелева, имеет место равенство $A' = A$ и τ_a является просто сдвигом на класс α коцикла a.

2. Как ни очевидны предложения 35 и 35′, они весьма полезны. Мы увидим, что именно они позволяют определить отношения эквивалентности, встречающиеся в различных „точных последовательностях когомологий“.

Упражнение. Пусть A — некоторая G-группа и $E(A)$ — множество классов (A, A)-главных однородных пространств. Показать, что определенный на $E(A)$ закон композиции задает на нем структуру группы и что эта группа действует на множестве $H^1(G, A)$. Если группа A абелева, то группа $E(A)$ является полупрямым произведением группы $H^1(G, A)$ на группу $\mathrm{Aut}(A)$. В общем случае показать, что $E(A)$ содержит в качестве подгруппы факторгруппу группы $\mathrm{Aut}(A)$ по подгруппе внутренних автоморфизмов, определенных элементами из A^G. Как определяется $E(A)$ с помощью коциклов?

5.4. Точная последовательность когомологий, ассоциированная с подгруппой

Пусть A и B — две G-группы и u: $A \to B$ — некоторый G-гомоморфизм. Этот гомоморфизм определяет отображение

$$v\colon H^1(G, A) \to H^1(G, B).$$

Пусть $\alpha \in H^1(G, A)$. Предположим, что мы хотим описать слой элемента α относительно отображения v, иначе говоря, множество $v^{-1}(v(\alpha))$. Выберем некоторый коцикл a, представляющий класс α, и обозначим через b его образ в B. Если положить $A' = {}_aA$ и $B' = {}_bB$, то u определяет, очевидно, гомоморфизм

$$u'\colon A' \to B',$$

который в свою очередь определяет отображение

$$v'\colon H^1(G, A') \to H^1(G, B').$$

Кроме того, имеет место следующая коммутативная диаграмма:

$$\begin{array}{ccc} H^1(G, A) & \xrightarrow{v} & H^1(G, B) \\ {\scriptstyle\tau_a}\uparrow & & \uparrow{\scriptstyle\tau_b} \\ H^1(G, A') & \xrightarrow{v'} & H^1(G, B') \end{array}$$

(где буквы τ_a и τ_b обозначают биекции, определенные в предыдущем пункте). Поскольку τ_b отображает нейтральный элемент из $H^1(G, B')$ в $v(\alpha)$, то отсюда следует, что

τ_a *является биекцией ядра отображения* v' *на слой* $v^{-1}(v(\alpha))$ *элемента* α. Другими словами, скручивание позволяет отобразить каждый слой отображения v в ядро некоторого другого отображения и эти ядра уже могут фигурировать в точных последовательностях (см. [CL] loc. cit.).

Применим это рассуждение в простейшем случае, когда A — подгруппа группы B.

Введем в рассмотрение однородное пространство B/A *левых классов смежности* относительно подгруппы A. Оно является G-множеством, и, следовательно, определено множество $H^0(G, B/A)$. Более того, если $x \in H^0(G, B/A)$, то прообраз X элемента x в B является (правым) главным однородным пространством над A. Обозначим его класс в группе $H^1(G, A)$ через $\delta(x)$. Определенный таким образом кограничный оператор δ обладает следующим свойством:

Предложение 36. *Последовательность пунктированных множеств*

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B)$$

точна.

Простейшее доказательство опирается на определение δ в терминах коциклов. Пусть $c \in (B/A)^G$. Выберем элемент b из группы B в классе c и положим $a_s = b^{-1} \cdot {}^s b$; класс получившегося коцикла и есть $\delta(c)$. Его определение показывает, что он когомологичен нулю в B и что каждый коцикл со значениями в A, когомологичный нулю в B, имеет такой вид. Отсюда следует предложение.

Следствие 1. *Ядро отображения* $H^1(G, A) \to H^1(G, B)$ *отождествляется с факторпространством пространства* $(B/A)^G$ *относительно действия группы* B^G.

Это отождествление осуществляется при помощи оператора δ; нужно показать, следовательно, что $\delta(c) = \delta(c')$ тогда и только тогда, когда существует элемент b из B^G, такой, что $bc = c'$, но это совсем просто.

Следствие 2. *Пусть* $\alpha \in H^1(G, A)$ *и* a — *некоторый коцикл, представляющий класс* α. *Элементы из* $H^1(G, A)$,

имеющие тот же образ в $H^1(G, B)$, что и α, находятся в биективном соответствии с элементами фактормножества множества $H^0(G, {}_aB/{}_aA)$ относительно действия группы $H^0(G, {}_aB)$.

Этот факт получается с помощью метода скручивания из следствия 1 аналогично тому, как это объяснялось выше.

Следствие 3. *Для того чтобы множество $H^1(G, A)$ было счетным (соответственно было конечным или состояло из одного элемента), необходимо и достаточно, чтобы таким же был его образ в $H^1(G, B)$ и все фактормножества $({}_aB/{}_aA)^G/({}_aB)^G$ для всех $a \in Z^1(G, A)$.*

Это вытекает из следствия 2.

Оказывается можно дать явное описание образа $H^1(G, A)$ в $H^1(G, B)$ [как если бы выражение $H^1(G, B/A)$ имело смысл!].

Предложение 37. *Пусть $\beta \in H^1(G, B)$ и $b \in Z^1(G, B)$ — некоторый представитель из класса β. Для того чтобы β принадлежал образу $H^1(G, A)$, необходимо и достаточно, чтобы пространство ${}_b(B/A)$, полученное из B/A скручиванием с помощью b, имело G-инвариантную точку.*

[В комбинации со следствием 2 предложения 36 это означает, что множество элементов из $H^1(G, A)$, имеющих в качестве образа элемент β, находится в биективном соответствии с фактормножеством $H^0(G, {}_b(B/A))/H^0(G, {}_bB)$.]

Для принадлежности элемента β образу $H^1(G, A)$ необходимо и достаточно существование такого элемента $b \in B$, что для каждого $s \in G$ элемент $b^{-1}b_s{}^sb$ принадлежит A. Обозначим через c образ элемента b в B/A, тогда предыдущее означает, что $c = b_s \cdot {}^sc$, иначе говоря, $c \in H^0(G, {}_b(B/A))$, что и требовалось доказать.

Замечание. Предложение 37 является аналогом следующей классической теоремы Эресмана: для того чтобы структурную группу главного расслоения можно было привести к ее подгруппе, необходимо и достаточно, чтобы расслоенное пространство, слоями которого являются соответствующие однородные пространства, имело некоторое сечение.

5.5. Точная последовательность когомологий, ассоциированная с нормальным делителем

Пусть A — нормальный делитель в группе B и положим $C = B/A$. В этом случае C является G-группой.

Предложение 38. *Последовательность пунктированных множеств*

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

точна.

Проверка проста (см. [CL], стр. 133).

Слои отображения $H^1(G, A) \to H^1(G, B)$ были описаны в п. 5.4. Однако то, что A является нормальным делителем в B, позволяет упростить это описание. Отметим прежде всего следующее.

Группа C^G естественно действует (справа) на множестве $H^1(G, A)$. В самом деле, пусть $c \in C^G$, и пусть $X(c)$ — полный прообраз элемента c в B. Тогда G-множество $X(c)$ снабжено естественной структурой (A, A)-главного однородного пространства. Если теперь P — произвольное главное однородное пространство над A, то композиция $P \circ X(c)$ также является главным однородным пространством над A; это и есть искомое действие. [Переведем сказанное на язык коциклов. Поднимая c до некоторого элемента $b \in B$, получаем, что ${}^s b = b \cdot x_s$, где $x_s \in A$. Каждому коциклу a_s со значениями в группе A сопоставим коцикл $b^{-1} a_s\, b x_s = b^{-1} a_s {}^s b$; его класс когомологий является образом класса (a_s) при действии c.]

Предложение 39. (i) *Если $c \in C^G$, то $\delta(c) = 1 \cdot c$, где 1 — нейтральный элемент из множества $H^1(G, A)$;*

(ii) *два элемента из $H^1(G, A)$ тогда и только тогда имеют один и тот же образ в $H^1(C, B)$, когда один переводится в другой с помощью некоторого элемента из C^G;*

(iii) *пусть $a \in Z^1(G, A)$ — коцикл, α — его образ в $H^1(G, A)$ и $c \in C^G$. Для справедливости равенства $\alpha \cdot c = \alpha$ необходимо и достаточно, чтобы элемент c принадлежал образу гомоморфизма $H^0(G, {}_aB) \to H^0(G, C)$.*

[$_aB$ обозначает группу, полученную скручиванием группы B с помощью коцикла a; разумеется, A действует на B внутренними автоморфизмами.]

Равенство $\delta(c) = 1 \cdot c$ следует из самого определения δ. С другой стороны, если два коцикла a_s и a'_s со значениями в A становятся когомологичными в группе B, то существует элемент $b \in B$, такой, что $a'_s = b^{-1} a_s\, {}^s b$. Пусть $c \in C$ — образ элемента b, тогда имеем ${}^s c = c$, откуда $c \in C^G$ и ясно, что c переводит класс коцикла a_s в класс коцикла a'_s. Обратное тривиально. Это доказывает (ii). Наконец, если $b \in B$ — некоторый прообраз элемента c и если $\alpha \cdot c = \alpha$, то существует элемент $x \in A$, такой, что $a_s = x^{-1} \cdot b^{-1} a_s\, {}^s b\, {}^s x$. Последнее равенство можно переписать в виде

$$bx = a_s\, {}^s(bx)\, a_s^{-1},$$

т. е. $bx \in H^0(G, {}_aB)$. Отсюда следует (iii).

Следствие 1. *Ядро отображения $H^1(G, B) \to H^1(G, C)$ отождествляется с фактормножеством множества $H^1(G, A)$ относительно действия группы C^G.*

Следствие 2. *Пусть $\beta \in H^1(G, B)$ и b — представляющий его коцикл. Элементы из $H^1(G, B)$, имеющие тот же образ в $H^1(G, C)$, что и элемент β, находятся в биективном соответствии с элементами фактормножества множества $H^1(G, {}_bA)$ относительно действия группы $H^0(G, {}_bC)$.*

[Группа B действует на себе внутренними автоморфизмами и оставляет группу A на месте, что позволяет осуществить *скручивание* точной последовательности $1 \to A \to B \to C \to 1$ с помощью коцикла b.]

Этот факт получается с помощью скручивания из следствия 1 точно так же, как это было объяснено в предыдущем пункте.

Замечание. Предложение 35 показывает, что множество $H^1(G, {}_bB)$ отождествляется с $H^1(G, B)$, а $H^1(G, {}_bC)$ — с $H^1(G, C)$. Напротив, множество $H^1(G, {}_bA)$ *не имеет, вообще говоря, никакой связи с* $H^1(G, A)$.

Следствие 3. *Для того чтобы множество $H^1(G, B)$ было счетным (соответственно было конечным или со-*

стояло из одного элемента), необходимо и достаточно, чтобы таким же был его образ в $H^1(G, C)$ и все фактормножества $H^1(G, {}_bA)/({}_bC)^G$, $b \in Z^1(G, B)$.

Это вытекает из следствия 2.

Упражнение. Показать, что сопоставление каждому $c \in C^G$ класса (A, A)-главных однородных пространств $X(c)$ определяет гомоморфизм группы C^G в группу $E(A)$, определенную в упражнении п. 5.3.

5.6. Случай абелева нормального делителя

Сохраняя обозначения предыдущего пункта, предположим, кроме того, что A — абелев нормальный делитель в группе B. Множество $H^1(G, A)$ является в этом случае абелевой группой, групповую операцию в которой мы будем записывать аддитивно. Пусть $\alpha \in H^1(G, A)$ и $c \in C^G$. Обозначим через α^c образ α при действии c, определение которого было дано выше. Опишем это действие более явно. Для этого заметим, что очевидный гомоморфизм $C^G \to \mathrm{Aut}(A)$ задает действие (слева) группы C^G на группе $H^1(G, A)$; образ α при действии c (относительно этого нового закона) будем обозначать через $c \cdot \alpha$.

Предложение 40. *Имеет место соотношение*

$$\alpha^c = c^{-1} \cdot \alpha + \delta(c),$$

где $\alpha \in H^1(G, A)$ *и* $c \in C^G$.

Доказательство состоит в следующем простом вычислении. Пусть $b \in B$ — какой-нибудь прообраз элемента c, тогда ${}^sb = b \cdot x_s$ и класс коцикла x_s совпадает с $\delta(c)$. С другой стороны, если a_s — коцикл в классе α, то в качестве представителя класса α^c можно взять коцикл $b^{-1}a_s\, {}^sb$, а в качестве представителя класса $c^{-1} \cdot \alpha$ — коцикл $b^{-1}a_sb$. Отсюда получается требуемая формула.

Следствие 1. *Имеет место равенство*

$$\delta(c'c) = \delta(c) + c^{-1} \cdot \delta(c').$$

Применяя предложение 40 к соотношению $\alpha^{c'c} = (\alpha^{c'})^c$, получаем указанную формулу.

Следствие 2. *Если A лежит в центре группы B, то отображение* $\delta\colon C^G \to H^1(G, A)$ *является гомоморфизмом и* $\alpha^c = \alpha + \delta(c)$.

Доказательство очевидно.

Покажем теперь, как применяется группа $H^2(G, A)$. A priori хотелось бы определить кограничный оператор

$$H^1(G, C) \to H^2(G, A).$$

В такой форме это возможно, лишь когда A содержится в центре группы B (см. п. 5.7). Однако справедлив следующий частичный результат.

Пусть $c \in Z^1(G, C)$ — некоторый коцикл со значениями в C. Поскольку группа A абелева, группа C *действует на* A и определена, следовательно, скрученная группа ${}_cA$. Мы хотим сопоставить коциклу c некоторый класс когомологий $\Delta(c) \in H^2(G, {}_cA)$. Для этого поднимем коцикл c_s до некоторого непрерывного отображения $s \to b_s$ группы G в группу B и составим выражение

$$a_{s,t} = b_s\, {}^s b_t b_{st}^{-1}.$$

Определенная таким образом двумерная коцепь является *коциклом* со значениями в ${}_cA$. Действительно, если принять во внимание способ действия G на ${}_cA$, то определение коцикла запишется в виде тождества

$$a_{s,t}^{-1} \cdot b_s\, {}^s a_{t,u} b_s^{-1} \cdot a_{s,tu} \cdot a_{st,u}^{-1} = 1.$$

Подставляя в него выражение для $a_{s,t}$, получаем

$$b_{st}\, {}^s b_t^{-1} b_s^{-1} \cdot b_s\, {}^s b_t\, {}^{st} b_u\, {}^s b_{tu}^{-1} b_s^{-1} \cdot b_s\, {}^s b_{tu} b_{stu}^{-1} \cdot b_{stu}\, {}^{st} b_u^{-1} b_{st}^{-1} = 1;$$

отсюда видно, что оно удовлетворяется (все члены сокращаются).

С другой стороны, если заменить b_s на $a'_s b_s$, то коцикл $a_{s,t}$ заменится на коцикл $a'_{s,t} \cdot a_{s,t}$, где

$$a'_{s,t} = (\delta a')_{s,t} = a'_s \cdot b_s\, {}^s a'_t b_s^{-1} \cdot a'^{-1}_{st};$$

последнее проверяется вычислениями, аналогичными предыдущим (и более простыми). Таким образом, класс коцикла $a_{s,t}$ определяется однозначно; его мы и возьмем за $\Delta(c)$.

Предложение 41. *Для того чтобы класс когомологий коцикла c принадлежал образу множества $H^1(G, B)$ в $H^1(G, C)$, необходимо и достаточно, чтобы $\Delta(c)$ был равен нулю.*

Необходимость очевидна. Обратно, если $\Delta(c) = 0$, то предыдущие рассуждения показывают, что можно найти коцикл b_s, для которого $b_s\,{}^s b_t b_{st}^{-1} = 1$ и образ b_s в C совпадает с c. Отсюда следует утверждение.

Следствие. *Если $H^2(G, {}_cA) = 0$ для каждого $c \in Z^1(G, C)$, то отображение $H^1(G, B) \to H^1(G, C)$ сюръективно.*

Упражнения. 1) Переформулировать предложение 40, используя упражнение п. 5.5, и установить, что $E(A)$ является полупрямым произведением группы $H^1(G, A)$ на группу $\mathrm{Aut}(A)$.

2) Пусть c и $c' \in Z^1(G, C)$ — два когомологичных коцикла. Сравнить $\Delta(c)$ и $\Delta(c')$.

5.7. Случай центральной подгруппы

Предположим теперь, что A лежит *в центре* группы B. Пусть $a = (a_s)$ — коцикл со значениями в группе A и $b = (b_s)$ — коцикл со значениями в B; тогда немедленно проверяется, что $a \cdot b = (a_s \cdot b_s)$ является коциклом со значениями в B. Более того, класс $a \cdot b$ зависит только от классов a и b. Отсюда заключаем, что абелева группа $H^1(G, A)$ *действует на множестве* $H^1(G, B)$.

Предложение 42. *Два элемента из $H^1(G, B)$ тогда и только тогда имеют одинаковый образ в $H^1(G, C)$, когда они переводятся друг в друга с помощью некоторого элемента из $H^1(G, A)$.*

Доказательство очевидно.

Пусть теперь $c \in Z^1(G, C)$. Так как C действует тривиально на A, то скрученная группа ${}_cA$, использовавшаяся в п. 5.6, канонически отождествляется с группой A и элемент $\Delta(c)$ принадлежит группе $H^2(G, A)$. Непосредственное вычисление показывает (см. [CL], стр. 132), что если коциклы c и c' когомологичны, то $\Delta(c) = \Delta(c')$. Таким образом, определено некоторое отображение

Δ: $H^1(G, C) \to H^2(G, A)$. Применяя предложения 38 и 41, получаем

Предложение 43. *Последовательность*

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \to$$
$$\to H^1(G, B) \to H^1(G, C) \xrightarrow{\Delta} H^2(G, A)$$

точна.

Как обычно, эта последовательность дает сведения только о ядре отображения Δ и ничего не говорит о соответствующем отношении эквивалентности. Для того чтобы его получить, нужно „скрутить“ рассматриваемые группы. Более точно, заметим, что C действует внутренними автоморфизмами на группе B и эти автоморфизмы тривиальны на A. Если $c = (c_s)$ — коцикл со значениями в C, то с помощью c можно скрутить точную последовательность $1 \to A \to B \to C \to 1$, в результате чего получится точная последовательность

$$1 \to A \to {}_cB \to {}_cC \to 1.$$

Отсюда получаем новый кограничный оператор

$$\Delta_c: H^1(G, {}_cC) \to H^2(G, A).$$

Поскольку, кроме того, имеется каноническая биекция

$$\tau_c: H^1(G, {}_cC) \to H^1(G, C),$$

то с ее помощью можно сравнить Δ и Δ_c. В результате получаем следующее

Предложение 44. *Имеет место соотношение*

$$\Delta \circ \tau_c(\gamma') = \Delta_c(\gamma') + \Delta(\gamma),$$

где $\gamma \in H^1(G, C)$ *обозначает класс коцикла* c, *а* γ' *пробегает все* $H^1(G, {}_cC)$.

Пусть c'_s — коцикл, представляющий класс γ'. Выберем, как и выше, некоторую коцепь b_s (соответственно b'_s) в B (соответственно в ${}_cB$), поднимающую коцикл c_s (соответственно c'_s). Тогда $\Delta(\gamma)$ можно представить коциклом

$$a_{s,t} = b_s\, {}^s b_t b_{st}^{-1},$$

а $\Delta_c(\gamma')$ — коциклом

$$a'_{s,t} = b'_s \cdot b_s\, {}^s b'_t b_s^{-1} \cdot b'^{-1}_{st}.$$

С другой стороны, $\tau_c(\gamma')$ можно задать коциклом $c'_s c_s$, поднятием которого является $b'_s b_s$. Следовательно, класс $\Delta \circ \tau_c(\gamma')$ представляется коциклом

$$a''_{s,t} = b'_s b_s \cdot {}^s b'_t\, {}^s b_t \cdot b_{st}^{-1} b'^{-1}_{st}.$$

Вычислим произведение $a'_{s,t} \cdot a_{s,t}$. Так как $a_{s,t}$ лежит в центре группы B, то можно написать

$$a'_{s,t} \cdot a_{s,t} = b'_s b_s\, {}^s b'_t b_s^{-1} \cdot a_{s,t} \cdot b'^{-1}_{st}.$$

Подставляя в правой части вместо $a_{s,t}$ его выражение и сокращая, получаем точно такое же выражение, как и для $a''_{s,t}$. Отсюда следует предложение.

Следствие. *Элементы из $H^1(G, C)$, имеющие при отображении Δ одинаковый образ γ, находятся в биективном соответствии с элементами фактормножества множества $H^1(G, {}_cB)$ относительно действия группы $H^1(G, A)$.*

В самом деле, биекция τ_c^{-1} отображает все эти элементы на элементы ядра отображения

$$\Delta_c\colon H^1(G, {}_cC) \to H^2(G, A).$$

Но предложения 42 и 43 показывают, что это ядро отождествляется с фактормножеством множества $H^1(G, {}_cB)$ относительно действия $H^1(G, A)$.

Замечания. 1. Множество $H^1(G, {}_cB)$ не находится, вообще говоря, в биективном соответствии с множеством $H^1(G, B)$.

2. Оставляем читателю сформулировать критерий счетности, конечности и т. д., который вытекает из предыдущего следствия.

5.8. Дополнения

Оставляем читателю самому проработать следующие пункты:

(а) Расширения групп. Пусть H — замкнутый нормальный делитель в G и A — некоторая G-группа. Факторгруппа G/H действует на A^H, что позволяет определить $H^1(G/H, A^H)$. С другой стороны, если $a_h \in Z^1(H, A)$ и $s \in G$, то можно определить преобразование $s(a)$ коцикла $a = (a_h)$ по формуле

$$s(a)_h = s\left(a_{s^{-1}hs}\right).$$

Переходя к когомологиям, получаем, что группа G действует на $H^1(H, A)$, и легко проверить, что при этом H действует тривиально. Можно говорить, следовательно, о *действии факторгруппы G/H на $H^1(H, A)$*, так же как и в абелевом случае. Имеет место точная последовательность

$$1 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A)^{G/H},$$

и отображение $H^1(G/H, A^H) \to H^1(G, A)$ инъективно.

(б) Индуцированные модули. Пусть H — замкнутая подгруппа в G и A — некоторая H-группа. Пусть $A^* = M_G^H(A)$ — группа непрерывных отображений a^*: $G \to A$, таких, что $a^*({}^h x) = {}^h a^*(x)$, $h \in H$, $x \in G$. Группа G действует на A^* по формуле $({}^g a^*)(x) = a^*(xg)$. Группа A^* становится, таким образом, G-группой, и имеют место канонические биекции

$$H^0(G, A^*) = H^0(H, A) \quad \text{и} \quad H^1(G, A^*) = H^1(H, A).$$

5.9. Одно свойство групп когомологической размерности, не превосходящей 1

Следующий результат должен был бы фигурировать в п. 3.4.

Предложение 45. *Пусть I — некоторое множество простых чисел. Предположим, что* $\mathrm{cd}_p(G) \leqslant 1$ *для каждого $p \in I$. Тогда группа G обладает свойством поднятия относительно расширений*

$$1 \to P \to E \to W \to 1,$$

где E — конечная группа, а порядок группы P не делится на простые числа, принадлежащие множеству I.

Доказательство будем проводить с помощью индукции по порядку группы P. Случай $\operatorname{Card}(P)=1$ тривиален. Предположим теперь, что $\operatorname{Card}(P)>1$, и пусть p — некоторый простой делитель $\operatorname{Card}(P)$. По предложению $p \notin I$. Пусть R—силовская p-подгруппа в P. Мы будем различать два случая:

(а) R — нормальный делитель в P. Тогда R является единственной силовской p-подгруппой в P и, следовательно, нормальным делителем в E. Имеем расширения

$$1 \to R \to E \to E/R \to 1,$$
$$1 \to P/R \to E/R \to W \to 1.$$

Так как $\operatorname{Card}(R/R) < \operatorname{Card}(P)$, то предположение индукции показывает, что гомоморфизм $f\colon G \to W$ поднимается до некоторого гомоморфизма $g\colon G \to E/R$. С другой стороны, поскольку R является p-группой, то из предложения 16, п. 3.4, следует, что g поднимается до гомоморфизма $h\colon G \to E$. Таким образом, поднят также и гомоморфизм f.

(б) R не является нормальным делителем в группе P. Пусть E' — нормализатор подгруппы R в E и P' — нормализатор R в P. Имеет место равенство $P' = E' \cap P$. С другой стороны, *образ* E' в W совпадает со всем W. Действительно, если $x \in E$, то ясно, что xRx^{-1} также является силовской p-подгруппой в P. В силу сопряженности силовских p-подгрупп, существует элемент $y \in P$, такой, что $xRx^{-1} = yRy^{-1}$. Тогда $y^{-1}x \in E'$. Это показывает, что $E = P \cdot E'$ и утверждение доказано. На основании этого мы имеем расширение

$$1 \to P' \to E' \to W \to 1.$$

Так как $\operatorname{Card}(P') < \operatorname{Card}(P)$, то предположение индукции показывает, что морфизм $f\colon G \to W$ поднимается до морфизма $h\colon G \to E'$, и так как E' — подгруппа группы E, то все доказано.

Следствие. *Всякое расширение группы G с помощью проконечной группы, порядок которой не делится на простые числа, принадлежащие I, тривиально.*

Случай когда группа P конечна, непосредственно выводится из предыдущего предложения и леммы 2, п. 1.2.

Переход к общему случаю осуществляется с помощью леммы Цорна, аналогично тому, как это делалось в п. 3.4.

Замечание. Предыдущее следствие дает новое доказательство известного факта, что расширение конечной группы A с помощью конечной группы B тривиально, когда порядки групп A и B взаимно просты (см. Цассенхауз [1], гл. IV, § 7).

Предложение 46. *В предположениях предложения* 45 *пусть*

$$1 \to A \to B \to C \to 1$$

— точная последовательность G-групп. Предположим, кроме того, что A — конечная группа и что всякое простое число, делящее порядок группы A, принадлежит множеству I. Тогда каноническое отображение $H^1(G, B) \to H^1(G, C)$ сюръективно.

Пусть (c_s) — коцикл группы G со значениями в C. Обозначим гомоморфизм $B \to C$ через π, и пусть E обозначает множество пар (b, s), $b \in B$, $s \in G$, таких, что $\pi(b) = c_s$. Снабдим множество E следующим законом композиции:

$$(b, s) \cdot (b', s') = (b \cdot {}^s b', ss').$$

Тот факт, что $c_{ss'} = c_s \cdot {}^s c_{s'}$, показывает, что $\pi(b \cdot {}^s b') = c_{ss'}$; это доказывает корректность предыдущего определения. Проверяется, что множество E, снабженное этим законом композиции и топологией, индуцированной топологией прямого произведения $B \times G$, является компактной группой. Имеют место очевидные морфизмы

$$A \to E \quad \text{и} \quad E \to C,$$

которые означают, что группа E есть *расширение группы C с помощью группы A*. В силу следствия предложения 46 это расширение тривиально. Существует, таким образом, непрерывное сечение $s \to e_s$, являющееся морфизмом группы G в E. Перепишем e_s в виде (b_s, s). Из того, что $s \to e_s$ — морфизм, следует, что b_s является *коциклом группы G со значениями в B*, который поднимает заданный коцикл c_s. Это доказывает предложение.

СЛЕДСТВИЕ. *Пусть* $1 \to A \to B \to C \to 1$ — *точная последовательность* G-*групп. Если* A *конечна и* $\mathrm{cd}(G) \leqslant 1$, *то отображение*

$$H^1(G, B) \to H^1(G, C)$$

сюръективно.

Это частный случай предложения, когда I является множеством всех простых чисел.

Упражнения. 1) Пусть $1 \to A \to B \to C \to 1$ — точная последовательность G-групп, где A — конечная группа. Как было показано в доказательстве предложения 46, с каждым коциклом $c \in Z^1(G,C)$ связывается расширение E_c группы G с помощью A. Показать, что соответствующее этому расширению действие G на A совпадает с действием G на группе ${}_cA$ и что образ E_c в $H^2(G, {}_cA)$ совпадает с элементом $\Delta(c)$, определенным в п. 5.6.

2) Пусть A — конечная G-группа, порядок которой взаимно прост с порядком группы G. Показать, что в этом случае $H^1(G, A) = 0$. [Свести к конечному случаю, где этот результат известен: он является следствием теоремы Фейта - Томсона, утверждающей, что группы нечетного порядка разрешимы.]

БИБЛИОГРАФИЧЕСКИЕ УКАЗАНИЯ К ГЛАВЕ I

Почти все результаты § 1, 2, 3, 4 принадлежат Тейту. Сам Тейт их не опубликовал, однако некоторые из них были записаны Ленгом, а также Дуади (семинар Бурбаки, доклад 189). Другие (а именно доказательства, приведенные в п. 4.5) сообщены мне непосредственно.

Исключения составляют п. 3.5 (дуализирующий модуль) и п. 4.4 (теорема Шафаревича).

Параграф 5 (неабелевы когомологии) взят из статьи Бореля — Серра (см. Борель, Серр [1]). Он непосредственно подсказан теорией неабелевых когомологий с коэффициентами в пучках. Особенно полезен в связи с этим был доклад Гротендика в Канзасе.

6 Зак. 1202

ДОПОЛНЕНИЕ
НЕКОТОРЫЕ ТЕОРЕМЫ ДВОЙСТВЕННОСТИ
(свободный перевод одного письма Тейта от 28/III 1963 г.)

...Ты был излишне осторожен, определяя дуализирующие модули: никаких предположений о конечности не нужно. Вообще пусть R — топологическое кольцо, открытые двусторонние идеалы которого образуют фундаментальную систему окрестностей нуля. Пусть I — такой идеал и M — некоторый R-модуль; положим $M_I = \operatorname{Hom}_R(R/I, M)$ — подмодуль M, образованный элементами, аннулируемыми идеалом I. Пусть $\mathscr{C}(R)$ — категория R-модулей, являющихся объединением таких подмодулей M_I. Пусть T: $\mathscr{C}(R)^0 \to (\mathrm{Ab})$ — контравариантный аддитивный функтор, переводящий индуктивные пределы в проективные. *Такой функтор T точен слева тогда и только тогда, когда он представим.* Если R дискретно, этот результат хорошо известен: отображение $M = \operatorname{Hom}_R(R, M) \to \operatorname{Hom}(T(M), T(R))$ определяет функторный морфизм

$$a_M\colon\ T(M) \to \operatorname{Hom}_R(M,\ T(R)),$$

который биективен, когда M свободен. Следовательно, он биективен и при произвольном M, если T точен слева (надо воспользоваться свободной резольвентой M).

В общем случае, если I — открытый двусторонний идеал в R, то категория $\mathscr{C}(R/I)$ является полной подкатегорией в $\mathscr{C}(R)$ и функтор вложения $\mathscr{C}(R/I) \to \mathscr{C}(R)$ точен и перестановочен с $\varinjlim$. Отсюда следует, что если функтор T точен слева, то таким же будет и его ограничение на $\mathscr{C}(R/I)$, и для любого $M \in \mathscr{C}(R/I)$ имеем функторный изоморфизм

$$T(M) \to \operatorname{Hom}_R(M,\ T(R/I)). \qquad (*)$$

Применяя это к модулю $M = R/I_0$, где $I_0 \supset I$, получаем равенство $T(R/I_0) = T(R/I)_{I_0}$. Положив $E = \lim\limits_{I \to 0} T(R/I)$,

получим, что $T(R/I_0) = E_{I_0}$; применяя формулу (*) к I_0, приходим к равенству

$$T(M) = \mathrm{Hom}_R(M,\ E) \quad \text{для всех} \quad M \in \mathscr{C}(R/I_0).$$

Наконец, если M — произвольный модуль, то

$$T(M) = \varprojlim T(M_{I_0}) = \varprojlim \mathrm{Hom}_R(M_{I_0},\ E) = \mathrm{Hom}_R(M,\ E).$$

Разумеется, для определения функторного морфизма a_M: $T(M) \to \mathrm{Hom}_R(M,\ E)$ достаточно аддитивности функтора T, и хорошая формулировка состоит в утверждении, что следующие три свойства эквивалентны:

(i) T точен слева, $T \circ \varinjlim = \varprojlim \circ T$;

(ii) T полуточен, функторный морфизм $T \circ \varinjlim \to \varprojlim \circ T$ сюръективен, а a_M инъективен для всех M;

(iii) морфизм a_M биективен для всех M.

* * *

Пусть теперь G — проконечная группа, $A \in \mathscr{C}_G$ и S — замкнутая подгруппа из G; положим

$$D_r(S,\ A) = \varinjlim_{V \supset S} H^r(V,\ A)^*,$$

где предел берется по открытым подгруппам V группы G, содержащим S, относительно гомоморфизмов Cor^*, сопряженных гомоморфизмам коограничения. [Напомним, что если B — абелева группа, то через B^* обозначается группа $\mathrm{Hom}(B,\ \mathbf{Q}/\mathbf{Z})$.] Группы $D_r(S,\ A)$ образуют контравариантный гомологический функтор: каждой точной последовательности $0 \to A' \to A \to A'' \to 0$ соответствует точная последовательность

$$\ldots \to D_r(S,\ A'') \to D_r(S,\ A) \to D_r(S,\ A') \to \\ \to D_{r-1}(S, A'') \to \ldots$$

Положим $D_r(A) = D_r(\{1\},\ A)$; так как группа G/U действует на $H^r(U,\ A)$, группа $D_r(A)$ принадлежит категории $\mathscr{C}_G$.

В частности, положим

$$E_r = D_r(\mathbf{Z}) = \varinjlim H^r(G, \mathbf{Z}[G/U])^*,$$

$$E'_r = \varinjlim_m D_r(\mathbf{Z}/m\mathbf{Z}) = \varinjlim_{U, m} H^r(G, (\mathbf{Z}/m\mathbf{Z})[G/U])^*.$$

Сказанное вначале можно применить к топологическим кольцам

$$R = \mathbf{Z}[G] = \varprojlim \mathbf{Z}[G/U] \quad \text{и} \quad R' = \hat{\mathbf{Z}}[G] = \varprojlim (\mathbf{Z}/m\mathbf{Z})[G/U].$$

Имеют место равенства $\mathscr{C}(R) = \mathscr{C}_G$, $\mathscr{C}(R') = \mathscr{C}_G^t$. Отсюда, приняв за T функтор $H^r(G, \ )^*$, получаем функторные морфизмы

$$a_M\colon H^r(G, M)^* \to \mathrm{Hom}_G(M, E_r) \quad \text{для} \quad M \in \mathscr{C}_G$$

и

$$a'_M\colon H^r(G, M)^* \to \mathrm{Hom}_G(M, E'_r) \quad \text{для} \quad M \in \mathscr{C}_G^t.$$

Так как функтор T переводит $\varinjlim$ в $\varprojlim$, получаем, что следующие три условия эквивалентны:

а) морфизм a_M биективен для всех $M \in \mathscr{C}_G$;
б) морфизм a_M инъективен для всех $M \in \mathscr{C}_G$;
в) $\mathrm{scd}(G) \leqslant r$.

Аналогичное утверждение справедливо, если заменить a_M на a'_M, $\mathscr{C}_G$ на $\mathscr{C}_G^t$ и $\mathrm{scd}(G)$ на $\mathrm{cd}(G)$.

Пусть теперь $\mathrm{cd}(G) \leqslant r$. Тогда

$$E_{r+1} = D_{r+1}(\mathbf{Z}) = D_r(\mathbf{Q}/\mathbf{Z}) = \varinjlim H^r(U, \mathbf{Q}/\mathbf{Z})^* =$$
$$= \varinjlim \mathrm{Hom}_U(\mathbf{Q}/\mathbf{Z}, E'_r) = \bigcup \mathrm{Hom}(\mathbf{Q}/\mathbf{Z}, E'_r)^U.$$

Таким образом, получаем твой критерий:

$\mathrm{scd}_p(G) = r+1 \Leftrightarrow (E'_r)^U$ содержит подгруппу, изоморфную $\mathbf{Q}_p/\mathbf{Z}_p$.

Пример. $G = \hat{\mathbf{Z}}$, $E'_1 = \mathbf{Q}/\mathbf{Z}$, откуда $E_2 = \mathrm{Hom}(\mathbf{Q}/\mathbf{Z}, \mathbf{Q}/\mathbf{Z}) = \hat{\mathbf{Z}}$. Следовательно, для всех $M \in \mathscr{C}_G$

$$H^2(G, M)^* = \mathrm{Hom}_G(M, \hat{\mathbf{Z}}).$$

Если $\mathrm{cd}(G) = \mathrm{scd}(G) = r$, то, разумеется, E'_r — максимальный периодический подмодуль модуля E_r. Например, если

$G = G(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$, то локальная теория полей классов показывает, что $E_2 = \varinjlim \hat{K}^*$, где $\hat{K}^*$ означает естественную компактификацию мультипликативной группы K^*, а поля K пробегают множество конечных расширений поля $\mathbf{Q}_p$. Группа $\mu = E_2'$ является максимальной периодической подгруппой в E_2.

* * *

Перейдем к *теореме двойственности*.

Следующий пустячок — это лучшее, что я смог сделать.

Определение. *Пусть* $A \in \mathscr{C}_G$; *мы пишем* $\operatorname{cd}(G, A) \leqslant n$, *если* $H^r(S, A) = 0$ *для всех* $r > n$ *и всех замкнутых подгрупп* $S \subset G$.

Лемма 1. *Пусть* $A \in \mathscr{C}_G$. *Следующие три условия эквивалентны*:

(i) $\operatorname{cd}(G, A) = 0$.

(ii) *Для любого открытого нормального делителя* U *группы* G G/U*-модуль* A^U *когомологически тривиален.*

(iii) *Для любой пары* U, V, *где* $V \supset U$, *образованной открытыми нормальными делителями группы* G, *гомоморфизм*

$$N\colon H_0(V/U, A^U) \to H^0(V/U, A^U),$$

определенный следом, биективен.

Эквивалентность (ii) и (iii) вытекает из теоремы 8, стр. 152, [CL], примененной к $q = -1$. С другой стороны, если выполняется (i), то спектральная последовательность

$$H^p(V/U, H^q(U, A)) \Rightarrow H^n(V, A)$$

вырождается; так как ее предел тривиален, получаем, что $H^p(V/U, A^U) = 0$ для всех $p \neq 0$, откуда следует условие (ii). Наоборот, если выполняется утверждение (ii), то

$$H^p(V, A) = \varinjlim H^p(V/U, A^U) = 0 \quad \text{для всех} \quad p \neq 0,$$

откуда $H^p(S, A) = \varinjlim_{V \supset S} H^p(V, A) = 0$ для любой замкнутой подгруппы S группы G, что доказывает условие (i).

Пусть теперь $A \in \mathscr{C}_G$ и

$$0 \to A \to X^0 \to X^1 \to \dots$$

— каноническая резольвента модуля A, например, задаваемая непрерывными однородными цепями (не обязательно „эквивариантными"). Пусть Z^n — группа коциклов из X^n. Имеем точную последовательность

$$0 \to A \to X^0 \to X^1 \to \ldots \to X^{n-1} \to Z^n \to 0. \qquad (1)$$

Лемма 2. *Следующие свойства эквивалентны*:

(i) $\operatorname{cd}(G, A) \leqslant n$;

(ii) $\operatorname{cd}(G, Z^n) = 0$.

Действительно, для всех $r \neq 0$

$$H^r(S, Z^n) = H^{r+1}(S, Z^{n-1}) = \ldots = H^{r+n}(S, A).$$

Теорема 1. *Если* $\operatorname{cd}(G, A) \leqslant n$, *то с любым открытым нормальным делителем* U *группы* G *ассоциируется спектральная последовательность гомологического типа*

$$E^2_{p,q} = H_p(G/U, H^{n-q}(U, A)) \Rightarrow H_{p+q} = H^{n-(p+q)}(G, A). \quad (2)$$

Кроме того, эта спектральная последовательность функториальна по U: если $V \subset U$, то соответствующий гомоморфизм $H_p(G/V, H^{n-q}(V, A)) \to H_p(G/U, H^{n-q}(U, A))$ индуцируется гомоморфизмами $G/V \to G/U$ и Cor: $H^{n-q}(V, A) \to H^{n-q}(U, A)$.

Следствие. *Если* $\operatorname{cd}(G, A) \leqslant n$, *то для любого замкнутого нормального делителя* N *группы* G *существует спектральная последовательность когомологического типа*

$$E_2^{p,q} = H^p(G/N, D_{n-q}(N, A)) \Rightarrow H^{n-(p+q)}(G, A)^*. \qquad (3)$$

В частности, для $N = \{1\}$

$$H^p(G, D_{n-q}(A)) \Rightarrow H^{n-(p+q)}(G, A)^*. \qquad (4)$$

Это следствие можно получить из теоремы 1, применяя функтор двойственности $(\quad)^*$, используя двойственность для когомологий конечных групп (т. е. формулу $H_p(G/U, B)^* = H^p(G/U, B^*)$, ср. [M], стр. 303, 304) и переходя к индуктивному пределу по подгруппам U, содержащим N.

Доказать саму теорему 1 не трудно. Рассмотрим комплекс

$$0 \to (X^0)^U \to (X^1)^U \to \ldots \to (X^{n-1})^U \to (Z^n)^U \to 0, \qquad (5)$$

полученный из последовательности (1). Перепишем его в гомологической форме

$$0 \to Y_n \to Y_{n-1} \to \ldots \to Y_1 \to Y_0 \to 0. \qquad (6)$$

Таким образом, $H_q(Y) = H^{n-q}(U, A)$ для всех q. Применим теперь к Y функтор „цепи относительно G/U“. Получим двойной комплекс гомологического типа

$$C_{p, q} = C_p(G/U, Y_q).$$

Переходя к гомологиям „по q“, получим, поскольку C_p — точный функтор, комплекс $C_p\big(G/U, H^{n-q}(U, A)\big)$. Беря затем гомологии по p, получим искомый член $H_p\big(G/U, H^{n-q}(U, A)\big) = E^2_{p, q}$. С другой стороны, если взять сначала гомологии по p, то получим группы $H_p(G/U, Y_q)$. Они равны нулю для $p \neq 0$ в силу лемм 1 и 2; эти же леммы показывают, что для $p = 0$

$$H_0(G/U, Y_q) = H^0(G/U, Y_q) = Y_q^{G/U} = \\ = \big((X^{n-q})^U\big)^{G/U} = (X^{n-q})^G.$$

Таким образом, получаем комплекс, (ко)гомологии которого равны $H^{n-q}(G, A)$, что нам и было нужно. Отсюда следует утверждение теоремы.

Приложения

Теорема 2. *Пусть G — проконечная группа и n — целое число, большее или равное 0. Следующие условия эквивалентны:*

(i) $\mathrm{scd}(G) = n$, *группа* $E_n = D_n(\mathbf{Z})$ *делима и* $D_q(\mathbf{Z}) = 0$ *для* $q < n$;

(ii) $\mathrm{scd}(G) = n$, $D_q(A) = 0$ *для любого* $q < n$, *если модуль* $A \in \mathscr{C}_G$ *конечного типа над* $\mathbf{Z}$;

(iii) $H^r(G, \mathrm{Hom}(A, E_n)) = H^{n-r}(G, A)^*$ *для всех* r *и всех* $A \in \mathscr{C}_G$ *конечного типа над* $\mathbf{Z}$.

Кроме того, имеет место

Теорема 3. *Следующие условия эквивалентны:*

(i) $\mathrm{cd}(G) = n$, $D_q(\mathbf{Z}/p\mathbf{Z}) = 0$ *для всех* $q < n$ *и любого простого числа* p;

(ii) $\operatorname{cd}(G) = n$, $D_q(A) = 0$ *для всех* $A \in \mathscr{C}_G^f$ *и* $q < n$;

(iii) $H^r(G, \operatorname{Hom}(A, E'_n)) = H^{n-r}(G, A)^*$ *для всех* r *и* $A \in \mathscr{C}_G^f$.

Заметим, что группа $D_1(\mathbf{Z})$ всегда нулевая и что $D_0(\mathbf{Z}) = 0$, если порядок G делится на p^∞ для всех p. Таким образом, если $\operatorname{scd}(G) = 2$, группа G удовлетворяет условиям теоремы 2 (для $n = 2$) в том и только том случае, когда группа E_2 делима. Например, это верно в случае $G(\mathbf{Q}_p/\mathbf{Q}_p)$. Однако это *не так* для $G(k/k)$, где k — чисто мнимое числовое поле[1]). Too bad ...

Вот одно приложение теоремы 3.

Если G — аналитическая про-p-группа, для которой $\operatorname{cd}_p(G) < \infty$, то приложима теорема двойственности (iii) [т. е. G — группа Пуанкаре в терминологии п. 4.5]. Действительно, как доказал Лазар, группа G содержит открытую подгруппу U, являющуюся группой Пуанкаре; так как D_q для групп U и G совпадают, получаем, что $D_q(\mathbf{Z}/p\mathbf{Z}) = 0$ для всех $q < n$, после чего применяем импликацию (i) $\Rightarrow$ (iii) [это рассуждение фактически доказывает следующее: если G — про-p-группа конечной когомологической размерности, содержащая открытую подгруппу, являющуюся группой Пуанкаре, то G также является группой Пуанкаре].

---

[1]) Определение см. далее стр. 101. — *Прим. ред.*

ГЛАВА II

КОГОМОЛОГИИ ГАЛУА КОММУТАТИВНЫЙ СЛУЧАЙ

§ 1. ОБЩИЕ РЕЗУЛЬТАТЫ

1.1. Когомологии Галуа

Пусть k — поле, а K — его расширение Галуа. Группа Галуа $G(K/k)$ расширения K/k является проконечной группой (ср. гл. I, п. 1.1), к которой можно применить технику и результаты гл. I; в частности, если $G(K/k)$ действует на дискретной группе $A(K)$, определены множества $H^q(G(K/k), \ A(K))$ (если $A(K)$ не коммутативна, то q принимает лишь значения 0 или 1).

Однако с фиксированным расширением K/k мы имеем дело редко, обычная ситуация такова:

Заданы *основное поле* k и *функтор* $K \longrightarrow A(K)$, определенный на категории сепарабельных алгебраических расширений поля k и принимающий значения в категории групп (соответственно абелевых групп). Этот функтор удовлетворяет следующим аксиомам:

(1) $A(K) = \varinjlim A(K_i)$, где K_i — подрасширения K конечного типа над k.

(2) Если $K \to K'$ — вложение, то соответствующий морфизм $A(K) \to A(K')$ инъективен.

(3) Если K/K' — расширение Галуа, то $A(K)$ отождествляется с $H^0(G(K'/K), \ A(K'))$.

(Последнее имеет смысл, так как группа $G(K'/K)$ по функториальности действует на $A(K')$. Кроме того, аксиома (1) показывает, что это действие непрерывно.)

Замечания. 1. Обозначим через k_s сепарабельное замыкание поля k; тогда определена группа $A(k_s)$, являющаяся $G(k_s/k)$-группой. Знание этой группы *эквивалентно* (с точностью до изоморфизма функторов) знанию функтора A.

2. Часто случается, что функтор A может быть определен *для всех расширений поля* k (не обязательно

алгебраических или сепарабельных) и для этого функтора выполняются аксиомы (1), (2) и (3). Самый важный пример доставляют „групповые схемы“ [1]). Если A — групповая схема локально конечного типа над k, то точки из A со значениями в расширении K/k образуют группу $A(K)$, функториально зависящую от K. Этот функтор удовлетворяет аксиомам (1), (2), (3) (выполнение аксиомы (1) следует из того, что A локально конечного типа). В частности, это относится к „алгебраическим группам“, т. е. к групповым схемам конечного типа над k [2]).

Пусть A — функтор, удовлетворяющий сформулированным выше аксиомам. Если K'/K — расширение Галуа, то определены множества $H^q(G(K'/K), A(K'))$ (если A не коммутативна, то значения q ограничиваются 0 или 1). Обозначим их через $H^q(K'/K, A)$.

Пусть K_1'/K_1 и K_2'/K_2 — расширения Галуа с группами Галуа G_1 и G_2. Предположим, что задано вложение i: $K_1 \to K_2$ и что существует продолжающее его вложение j: $K_1' \to K_2'$. Последнее определяет гомоморфизм $G_2 \to G_1$ и морфизм $A(K_1') \to A(K_2')$; эти два отображения совместимы и определяют отображения $H^q(G_1, A(K_1')) \to H^q(G_2, A(K_2'))$, *не зависящие от выбора* j (ср. [CL], стр. 164) [3]). Таким

---

[1]) Пусть $\mathscr{C}$ — категория, $\hat{\mathscr{C}}$ — категория контравариантных функторов на $\mathscr{C}$ со значением в категории групп. Объект X из $\mathscr{C}$ называется группой, если он представляет некоторый функтор из $\hat{\mathscr{C}}$, т. е. если задан подъем функтора $Y \longrightarrow \mathrm{Hom}(Y, X)$ до объекта $\hat{\mathscr{C}}$. В частности, если $\mathscr{C} = (\mathrm{Sch}/S)$—категория схем над базисной схемой S (см. Ж. Дьедонне [2*]), то группа в $\mathscr{C}$ называется групповой схемой над S. — *Прим. перев.*

[2]) Если говорить о классических алгебраических группах, то нужно еще требовать приведенность над k. — *Прим. перев.*

[3]) Приведем доказательство этого утверждения. Прежде всего, гомоморфизм $\bar{j}$: $G_2 \to G_1$ определяется следующим образом: если $s_2 \in G_2$, то $\bar{j}(s_2)$ есть однозначно определенный элемент $s_1 \in G_1$, для которого $j \circ s_1 = s_2 \circ j$. Совместимость морфизма $\bar{j}$ с морфизмом $A(K_1') \to A(K_2')$ проверяется очевидным образом. Для доказательства нужного нам утверждения заметим теперь, что два различных вложения j: $K_1' \to K_2'$ и j': $K_1' \to K_2'$ отличаются на элемент $g \in G_1$. Это показывает, что $\bar{j}' = \sigma_g \circ \bar{j}$, где σ_g — внутренний автоморфизм группы G, определяемый элементом g. Остается,

образом, имеем отображения

$$H^q(K'_1/K_1, A) \to H^q(K'_2/K_2, A),$$

зависящие только от i (и от *существования* j).

В частности, мы видим, что различные сепарабельные замыкания поля k определяют группы $H^q(k_s/k, A)$, находящиеся в каноническом биективном соответствии. Это позволяет отбросить символ k_s и писать просто $H^q(k, A)$. Группы $H^q(k, A)$ функториально зависят от k.

1.2. Первые примеры

Пусть $\mathbf{G}_a$ (соответственно $\mathbf{G}_m$) — аддитивная (соответственно мультипликативная) групповая схема, определяемая соотношением $\mathbf{G}_a(K) = K^+$ (соответственно $\mathbf{G}_m(K) = K^*$). Имеет место (ср. [CL], стр. 158) [1])

следовательно, показать, что канонический гомоморфизм когомологий групп

$$H^q(G, A) \to H^q(G, A),$$

индуцированный внутренним автоморфизмом группы G, всегда тождествен. Для $q = 0$ это очевидно. С другой стороны, σ_g индуцирует автоморфизм ∂ функтора $H^q(G, \cdot)$, тождественный для $q = 0$. Согласно общему результату (см. Гротендик [1], гл. 2, п. 2. 3), отсюда следует, что этот автоморфизм тождествен для всех q. — *Прим. перев.*

[1]) Первое утверждение предложения известно под названием „теоремы 90" Гильберта и доказывается следующим образом: пусть K/k — конечное расширение поля k, и пусть $\{a_s\}_{s \in G}$ есть 1-коцикл. Для $c \in K$ образуем „сумму Пуанкаре"

$$b = \sum_{s \in G} a_s c^s.$$

Теорема о линейной независимости автоморфизмов (Бурбаки [3*], гл. 5, § 7, п. 5) показывает, что можно выбрать $c \in K$ таким, что $b \neq 0$. С другой стороны, для любого $t \in G$

$$b^t = \sum_{s \in G} a_s^t c^{st} = \sum_{s \in G} a_t^{-1} a_{st} c^{st} = a_t^{-1} \cdot b,$$

что показывает, что $\{a_s\}$ — кограница.

Для доказательства второго утверждения воспользуемся теоремой о нормальном базисе (Бурбаки [3*], гл. 5, § 10, п. 8). Существует $c \in K$, такой, что для любого $a \in K$

$$a = \sum_{s \in G} a_s c^s, \quad \text{где} \quad a_s \in k.$$

Предложение 1. *Для любого расширения Галуа $K|k$ имеют место равенства $H^1(K|k, \mathbf{G}_m)=0$ и $H^q(K|k, \mathbf{G}_a)=0$, $q \geqslant 1$.*

Действительно, когда расширение $K|k$ *конечно*, группы когомологий Тейта [1]) $\hat{H}^q(K|k, \mathbf{G}_a)$ равны нулю для всех $q \in \mathbf{Z}$.

Замечание. Группы $H^q(K|k, \mathbf{G}_m)$ в общем случае ненулевые для $q \geqslant 2$. Напомним, что группа $H^2(K|k, \mathbf{G}_m)$ отождествляется с множеством элементов *группы Брауэра* $\mathrm{Br}(k)$, распадающихся над K; в частности, $H^2(k, \mathbf{G}_m) = \mathrm{Br}(k)$, ср. [CL], гл. 10 [2]).

§ 2. КРИТЕРИИ КОГОМОЛОГИЧЕСКОЙ РАЗМЕРНОСТИ

В следующих параграфах мы обозначаем через G_k группу Галуа расширения $k_s|k$, где k_s — сепарабельное замыкание k. Эта группа определена неоднозначно, с точностью до измоорфизма.

Для всякого простого числа p обозначим через $G_k(p)$ максимальную факторгруппу группы G_k, являющуюся про-

---

Это позволяет определить гомоморфизмы G-модулей

$$g: K^+ \to \mathbf{Z}(G) \otimes k^+ \quad \text{и} \quad h: \mathbf{Z}(G) \otimes k^+ \to k^+,$$

полагая

$$g(a) = \sum_{s \in G} s \otimes a_s \quad \text{и} \quad h\Big(\sum_{s \in G} s \otimes a_s\Big) = \sum a_s c^s$$

(группа $\mathbf{Z}(G) \otimes k^+$ рассматривается здесь как G-модуль, операторы на котором действуют как $g(s \otimes a) = gs \otimes a$). Легко видеть, что эти гомоморфизмы обратны друг другу и, следовательно, определяют изоморфизм $K^+ \simeq \mathbf{Z}(G) \otimes k^+$. Вспоминая определение индуцированного модуля, получаем, что K^+ индуцирован с единичной подгруппы, а следовательно, в силу предложения 10 гл. I группы когомологий его тривиальны. — *Прим. перев.*

[1]) Определение когомологий Тейта (или модифицированных когомологий групп) см. [M], стр. 289. — *Прим. перев.*

[2]) Определение группы Брауэра смотри также в книге Бурбаки [4*], гл. 8, § 10, п. 4. О когомологической интерпретации этой группы с помощью системы факторов см., например, Ван дер Варден [1*], § 133. — *Прим. перев.*

p-группой; группа $G_k(p)$ есть группа Галуа расширения $k_s(p)/k$; это расширение называется *максимальным p-расширением* поля k. Мы дадим некоторые критерии, позволяющие вычислять когомологическую размерность групп G_k и $G_k(p)$, ср. гл. I, § 3.

2.1. Один вспомогательный результат

Предложение 2. *Пусть G — проконечная группа, а $G(p) = G/N$ — наибольшая факторгруппа G, являющаяся про-p-группой. Предположим, что $\mathrm{cd}_p(N) \leqslant 1$. Тогда каноническое отображение*

$$H^q(G(p), \mathbf{Z}/p\mathbf{Z}) \to H^q(G, \mathbf{Z}/p\mathbf{Z})$$

является изоморфизмом. В частности, $\mathrm{cd}(G(p)) \leqslant \leqslant \mathrm{cd}_p(G)$.

Пусть N/M — максимальная факторгруппа N, являющаяся про-p-группой. Легко видеть, что M — нормальный делитель в группе G и что G/M — про-p-группа. Отсюда получаем, используя определение группы $G(p)$, что $M = N$. Таким образом, каждый морфизм N в p-группу тривиален. В частности, $H^1(N, \mathbf{Z}/p\mathbf{Z}) = 0$. С другой стороны, поскольку $\mathrm{cd}_p(N) \leqslant 1$, то $H^i(N, \mathbf{Z}/p\mathbf{Z}) = 0$ для $i \geqslant 2$. Спектральная последовательность Хохшильда — Серра показывает тогда, что гомоморфизм

$$H^q(G/N, \mathbf{Z}/p\mathbf{Z}) \to H^q(G, \mathbf{Z}/p\mathbf{Z})$$

является изоморфизмом для всех $q \geqslant 0$ [1]). Неравенство $\mathrm{cd}(G/N) \leqslant \mathrm{cd}_p(G)$ следует из предложения 21 гл. I.

Упражнение. В условиях предложения 2 пусть A есть p-периодический $G(p)$-модуль. Показать, что каноническое отображение $H^q(G(p), A) \to H^q(G, A)$ есть изоморфизм для всех $q \geqslant 0$.

---

[1]) Действительно, спектральная последовательность Хохшильда — Серра индуцирует точную последовательность когомологий (см. [M], стр. 395)

$$0 \to H^q(G/H, M^H) \to H^q(G, M) \to H^0(G/H, H^q(H, M^H)) \to \ldots .$$

Применяя ее к модулю $\mathbf{Z}/p\mathbf{Z}$ и пользуясь тем, что $H^i(N, \mathbf{Z}/p\mathbf{Z}) = 0$, $i > 0$, получаем то, что нужно. — *Прим. перев.*

2.2. Случай, когда p совпадает с характеристикой

Предложение 3. *Если k — поле характеристики p, то* $\mathrm{cd}_p(G_k) \leqslant 1$ *и* $\mathrm{cd}(G_k(p)) \leqslant 1$.

Положим $f(x) = x^p - x$. Отображение f аддитивно и определяет точную последовательность

$$0 \to \mathbf{Z}/p\mathbf{Z} \to \mathbf{G}_a \xrightarrow{f} \mathbf{G}_a \to 0.$$

Действительно, точность этой последовательности означает (по определению), что последовательность абелевых групп

$$0 \to \mathbf{Z}/p\mathbf{Z} \to k_s \xrightarrow{f} k_s \to 0$$

точна, что легко проверить. Переходя к когомологиям, получаем точную последовательность

$$H^1(k, \mathbf{G}_a) \to H^2(k, \mathbf{Z}/p\mathbf{Z}) \to H^2(k, \mathbf{G}_a).$$

В силу предложения 1 $H^2(k, \mathbf{Z}/p\mathbf{Z}) = 0$, т. е. $H^2(G, \mathbf{Z}/p\mathbf{Z}) = 0$. Этот результат применим также к замкнутым подгруппам G_k (поскольку они являются группами Галуа) и, в частности, к силовским p-подгруппам. Если H — такая группа, то, следовательно, $\mathrm{cd}(H) \leqslant 1$ (ср. гл. I, предложение 21), откуда $\mathrm{cd}_p(G_k) \leqslant 1$ (гл. I, следствие 1 к предложению 14).

Пусть N — ядро отображения $G_k \to G_k(p)$; предыдущее рассуждение можно применить к N и получить, что $\mathrm{cd}_p(N) \leqslant 1$. Предложение 2 показывает тогда, что $\mathrm{cd}(G_k(p)) \leqslant \mathrm{cd}_p(G_k) \leqslant 1$, что и требовалось доказать.

Следствие 1. *Группа $G_k(p)$ является свободной про-p-группой.*

Это вытекает из следствия 2 к предложению 24 гл. I. (Так как группа $H^1(G_k(p))$ отождествляется с $k/f(k)$, можно даже вычислить ранг этой группы.)

Следствие 2 (А л ь б е р т — Х о х ш и л ь д). *Если k' — радикальное расширение поля k, то каноническое отображение* $\mathrm{Br}(k) \to \mathrm{Br}(k')$ *сюръективно.*

Пусть k'_s — сепарабельное замыкание поля k', содержащее k_s. Так как расширение k'/k радикально, группу G_k можно отождествить с группой Галуа расширения k'_s/k'. Имеют место равенства

$$\mathrm{Br}(k) = H^2(G_k, k_s^*), \qquad \mathrm{Br}(k') = H^2(G_k, k_s'^*).$$

Кроме того, для любого $x \in k'_s$ существует такая степень q числа p, что $x^q \in k_s$; другими словами, группа k'^*_s / k^*_s является p-периодической. Поскольку $\mathrm{cd}_p(G_k) \leqslant 1$, то $H^2(G_k, k'^*_s / k^*_s) = 0$ и точная когомологическая последовательность показывает, что отображение $H^2(G_k, k^*_s) \to \to H^2(G_k, k'^*_s)$ сюръективно, что и требовалось доказать.

Замечание. В случае когда k' — радикальное расширение поля k высоты 1, ядро отображения $\mathrm{Br}(k) \to \to \mathrm{Br}(k')$ можно вычислить с помощью когомологий p-алгебры Ли дифференцирований поля k' над k, ср. Хохшильд [1].

2.3. Случай, когда p не совпадает с характеристикой

Предложение 4. *Пусть k — поле характеристики p, n — целое число, большее или равное* 1. *Следующие условия эквивалентны*:

(i) $\mathrm{cd}_p(G_k) \leqslant n$;

(ii) *для любого алгебраического расширения K поля k $H^{n+1}(K, \mathbf{G}_m)(p) = 0$ и группа $H^n(K, \mathbf{G}_m)$ является p-делимой*;

(iii) *то же утверждение, что и в* (ii), *для конечных сепарабельных расширений K/k степени, взаимно простой с p*.

(Напомним, что для абелевой периодической группы A символом $A(p)$ обозначается p-примарная компонента A.)

Обозначим через μ_p группу корней p-й степени из 1; эта группа содержится в k_s. Имеет место точная последовательность

$$0 \to \mu_p \to \mathbf{G}_m \xrightarrow{p} \mathbf{G}_m \to 0,$$

где символ „p" означает возведение в p-ю степень в группе $\mathbf{G}_m$. Заметим, что группа μ_p изоморфна $\mathbf{Z}/p\mathbf{Z}$ (как абелева группа — в общем случае G_k действует нетривиально на μ_p). Точная когомологическая последовательность показывает, что условие (ii) эквивалентно равенству $H^{n+1}(K, \mu_p) = 0$ для всех K; аналогичное утверждение справедливо для (iii).

Предположим теперь, что $\mathrm{cd}_p(G_k) \leqslant n$. Так как G_k изоморфна замкнутой подгруппе группы G_k, получаем, что $\mathrm{cd}_p(G_K) \leqslant n$, откуда $H^{n+1}(K, \mu_p) = 0$. Таким образом, (i) $\Rightarrow$ (ii). Импликация (ii) $\Rightarrow$ (iii) тривиальна. Предположим теперь, что выполняется (iii). Пусть H — силовская p-подгруппа группы G_k и K/k — соответствующее ей расширение. Тогда

$$K = \varinjlim K_i,$$

где K_i — конечные сепарабельные расширения k степени, взаимно простой с p. В силу условия (iii) $H^{n+1}(K_i, \mu_p) = 0$ для всех i, откуда $H^{n+1}(K, \mu_p) = 0$, т. е. $H^{n+1}(k, \mu_p) = 0$. Однако H является про-p-группой и, следовательно, может действовать на μ_p только тривиально; таким образом, группу μ_p можно отождествить с $\mathbf{Z}/p\mathbf{Z}$ и предложение 21 гл. I показывает, что $\mathrm{cd}(H) \leqslant n$, откуда следует утверждение (i), что и требовалось.

§ 3. ПОЛЯ, РАЗМЕРНОСТЬ КОТОРЫХ НЕ ПРЕВОСХОДИТ 1

3.1. Определение

Предложение 5. *Пусть k — поле. Следующие условия эквивалентны:*

(i) *имеет место неравенство* $\mathrm{cd}(G_k) \leqslant 1$; *кроме того, если поле k характеристики $p \neq 0$, то* $\mathrm{Br}(K)(p) = 0$ *для любого алгебраического расширения K/k;*

(ii) $\mathrm{Br}(K) = 0$ *для любого алгебраического расширения K/k;*

(iii) *если L/K — конечное расширение Галуа и K алгебраично над k, то $G(L/K)$-модуль L^* когомологически тривиален* [1]);

(iv) *в условиях* (iii) *норменное отображение $N_{L/K}$: $L^* \to K^*$ сюръективно.*

---

[1]) G — модуль A называется когомологически тривиальным, если для любого $n \in \mathbf{Z}$ $H^n(G, A) = 0$. — *Прим. перев.*

Условия (i′), (ii′), (iii′), (iv′) — *те же формулировки, что и* (i) — (iv), *только ограничиваемся конечными сепарабельными расширениями* K/k.

Эквивалентности (i)$\Leftrightarrow$(i′), (ii)$\Leftrightarrow$(ii′) следуют из теоремы Альберта — Хохшильда, доказанной в п. 2.2. Импликации (i)$\Leftrightarrow$(ii) следуют из предложений 3 и 4. Эквивалентности

$$(ii')\Leftrightarrow(iii')\Leftrightarrow(iv')$$

доказаны в [CL], стр. 169[1]). С другой стороны, если поле k удовлетворяет условию (ii), то этому же условию удовлетворяет также любое его алгебраическое расширение, которое, следовательно, удовлетворяет и условиям (ii′) и (iii′). Значит, для поля k выполняется условие (iii). Аналогичное рассуждение доказывает равносильность (ii)$\Leftrightarrow$(iv), что и требовалось доказать.

Замечание. Как отметил М. Ауслендер, для выполнения условий (i) — (iv) одного условия $\mathrm{Br}(k)=0$ недостаточно. Действительно, пусть k_0 — поле характеристики нуль, алгебраически незамкнутое, размерности 1 и не имеющее никаких нетривиальных абелевых расширений (например, максимальное разрешимое расширение поля $\mathbf{Q}$). Положим $k=k_0((T))$. Тогда $\mathrm{Br}(k)=0$, ср. [CL], теорема 2, стр. 194, и легко видеть, что существует конечное расширение k' поля k, для которого $\mathrm{Br}(k')\neq 0$; следовательно, $\dim(k)\geqslant 2$.

Определение. *Говорят, что поле k имеет размерность, не превосходящую* 1, *если оно удовлетворяет эквивалентным условиям предложения* 5.

---

[1]) Докажем эти эквивалентности. (iii′)$\Rightarrow$(iv′) следует из определения групп $\hat{H}$, так как $\hat{H}^0(G, L^*)=0$. Аналогично, так как $\hat{H}^2(G, L^*)=0$, переходя к пределу по расширениям Галуа L, получаем (iii′)$\Rightarrow$(ii′). Наоборот, предположим, что выполнено (i′) (соответственно (iii′)). Для любой подгруппы $H\subset G$ тогда $\hat{H}^2(H, L^*)=0$ (соответственно $\hat{H}^0(H, L^*)=0$). Так как, с другой стороны, в силу предложения 1 $H^1(H, L^*)=0$, искомая импликация вытекает из следующего общего результата: G-модуль A когомологически тривиален тогда и только тогда, когда для любой силовской подгруппы p-подгруппы $G_p\subset G$ $H^q(G_p, A)=0$ для двух соседних целых чисел q (см. [CL]). — *Прим. перев.*

7 Зак 1202

Мы пишем тогда $\dim(k) \leqslant 1$.

Предложение 6. (а) *Любое алгебраическое расширение поля размерности, не превосходящей* 1, *имеет также размерность, не превосходящую* 1.

(б) *Пусть k — совершенное поле. Для того чтобы* $\dim(k) \leqslant 1$, *необходимо и достаточно, чтобы* $\mathrm{cd}(G_k) \leqslant 1$.

Утверждение (а) тривиально. Для доказательства (б) заметим, что если поле k совершенно, то отображение $x \to x^p$ является биекцией k_s^* на себя; отсюда следует, что p-компонента группы $H^q(k, \mathbf{G}_m)$ равна нулю, в частности $\mathrm{Br}(k)(p) = 0$. Так как это рассуждение можно применить к любому алгебраическому расширению K/k, мы видим, что условие (i) предложения 5 сводится к условию $\mathrm{cd}(G_k) \leqslant 1$, что и требовалось доказать.

Предложение 7. *Пусть k — поле,* $\dim(k) \leqslant 1$ *и p — простое число. Тогда* $\mathrm{cd}(G_k(p)) \leqslant 1$.

Пусть $G_k(p) = G_k/N$. Так как $\mathrm{cd}(G_k) \leqslant 1$, то $\mathrm{cd}(N) \leqslant 1$ и предложение 2 показывает, что $\mathrm{cd}(G_k/N) \leqslant \mathrm{cd}_p(G_k)$, откуда следует утверждение.

3.2. Связь со свойством (C_1)

Это свойство формулируется следующим образом:

(C_1) *Любое уравнение $f(x_1, \ldots, x_n) = 0$, где f — однородный многочлен степени $d < n$ с коэффициентами в поле k, имеет нетривиальное решение в k^n.*

Мы увидим примеры таких полей в п. 3.3.

Предложение 8. *Пусть k — поле, удовлетворяющее условию* (C_1). Тогда:

(а) *каждое алгебраическое расширение k' поля k также удовлетворяет* (C_1);

(б) *если L/K — конечное расширение и K алгебраично над k, то $N_{L/K}(L^*) = K^*$.*

Для доказательства утверждения (а) можно предположить, что расширение k' конечно над k. Пусть $F(x)$ — однородный многочлен степени d от n переменных с коэффициентами из k'. Положим $f(x) = N_{k'/k}F(x)$; возьмем базис $e_1, \ldots, e_m$ расширения k'/k и выразим x через этот базис. Тогда f отождествляется с однородным многочле-

ном степени dm от nm переменных с коэффициентами из k. Если $d < n$, то $dm < nm$ и x является нулем этого многочлена. Это означает, что $N_{k'/k}F(x) = 0$, откуда $F(x) = 0$.

Предположим теперь, что мы находимся в условиях утверждения (б), и пусть $a \in K^*$. Положим $d = [L:K]$ и рассмотрим уравнение

$$N(x) = ax_0^d, \quad \text{где} \quad x \in L, \quad x_0 \in K.$$

Это однородное уравнение степени d от $d+1$ переменных. Так как в силу (а) поле K удовлетворяет условию (C_1), это уравнение имеет нетривиальное решение (x, x_0). Если бы x_0 был нулем, то $N(x)$ равнялся бы нулю, откуда $x = 0$ — противоречие. Таким образом, $x_0 \neq 0$ и $N(x/x_0) = a$, что доказывает сюръективность нормы.

Следствие. *Если поле k удовлетворяет условию* (C_1), *то* $\dim(k) \leqslant 1$ *и степень* $[k:k^p]$ *равна* 1 *или* p.

Предыдущее предложение показывает, что поле k удовлетворяет условию (iv) предложения 5. Таким образом, $\dim(k) \leqslant 1$. С другой стороны, предположим, что $k \neq k^p$, и пусть K — радикальное расширение поля k степени p. Согласно предыдущему предложению, $N(K) = k$. Но $N(K) = K^p$. Следовательно, $K^p = k$, откуда $K^{p^2} = k^p$ и $[k:k^p] = [K:K^p] = p$.

Замечания. 1. Соотношение „$[k:k^p] = 1$ или p“ можно выразить по-другому, сказав, что любое радикальное расширение k имеет вид $k^{p^{-i}}$, где $i = 0, 1, \ldots, \infty$.

2. Дж. Акс [1] доказал, что обращение следствия неверно: существует поле k характеристики нуль и размерности 1, не удовлетворяющее условию (C_1). Чтобы построить его, рассмотрим сначала поле k_0 характеристики нуль, содержащее корни из единицы и такое, что группа Галуа $G(\bar{k}_0/k_0)$ изоморфна $\mathbf{Z}_2 \times \mathbf{Z}_3$. Легко построить однородный многочлен $f(X, Y)$ степени 5 с коэффициентами в k_0, который не представляет нуль. Пусть $k_1 = k_0((T))$, и пусть k — поле, полученное присоединением к k_1 корней степени n из T для всех n, не делящихся на 5. Тогда

$$G(\bar{k}/k) = \mathbf{Z}_5 \times G(\bar{k}_0/k_0) = \mathbf{Z}_5 \times \mathbf{Z}_2 \times \mathbf{Z}_3,$$

так что $\dim(k) = 1$. С другой стороны, многочлен

$$F(X_1, \ldots, X_5; Y_1, \ldots, Y_5) = \sum_{i=1}^{5} T^i f(X_i, Y_i)$$

имеет степень 5 и не представляет нуля. Поэтому k не обладает свойством (C_1).

Аналогично, но сложнее Акс строит даже поле k размерности 1, не удовлетворяющее условию (C_r)[1]) ни для какого r.

Упражнение. Построить поле k, для которого $\dim(k) \leqslant 1$ и $[k : k'] > p$.

3.3. Примеры полей размерности, не превосходящей 1

(а) *Конечное поле* — поле типа (C_1) (теорема Шевалле[2])). В частности, оно имеет размерность, не превосходящую 1.

(б) Расширение степени трансцендентности 1 алгебраически замкнутого поля есть поле типа (C_1) (теорема Тзена[3])). В частности, ... и т. д.

(в) Пусть K — поле с дискретным нормированием, поле вычетов которого алгебраически замкнуто. Предположим, что K *гензелево*[4]) и что $\hat{K}$ *сепарабельно* над K. Тогда K удовлетворяет условию (C_1) (теорема Ленга [1]). В частности, это относится к максимальному неразветвленному расширению локального поля с совершенным полем вычетов.

(г) Пусть k — алгебраическое расширение поля $\mathbf{Q}$. Запишем $k = \varinjlim k_i$, где k_i конечны над $\mathbf{Q}$, и обозначим

---

[1]) См. ниже п. 4.5. — *Прим. перев.*

[2]) См. Боревич, Шафаревич [1*], стр. 15. — *Прим. перев.*

[3]) См. Ленг [1]. — *Прим. перев.*

[4]) То есть K является полем частных гензелева кольца. Коммутативное локальное кольцо называется гензелевым, если для него выполняется лемма Гензеля: если $f \in A[t]$ — унитарный многочлен с коэффициентами в A, $\bar{a} \in A/\mathfrak{m}A$ ($\mathfrak{m}$ — максимальный идеал A)—простой корень полинома $\bar{f} \in A/\mathfrak{m}A[t]$ (образа f при каноническом гомоморфизме $A[t] \to A/\mathfrak{m}A[t]$), то f имеет корень a, индуцирующий $\bar{a}$. Например, полное локальное кольцо (в частности, кольцо p-адических чисел, кольцо формальных степенных рядов) гензелево. О теории таких колец см. Гротендик [4], гл. 4, № 32, 1967. — *Прим. перев.*

через V_i множество „точек" поля k_i („точку" числового поля можно определить как топологию на этом поле, определяемую нетривиальным нормированием). Пусть $V = \varprojlim V_i$. Если $v \in V$, то точка v индуцирует точку на каждом поле k_i и определяет тем самым пополнение $(k_i)_v$. Положим

$$n_v(k) = \text{НОК}\,[(k_i)_v : \mathbf{Q}_v].$$

Это „сверхнатуральное" число (ср. гл. I, п. 1.3) называется *степенью поля k в точке v*.

Предложение 9. *Пусть k — алгебраическое расширение поля $\mathbf{Q}$ и p — простое число. Предположим, что $p \neq 2$ или что поле k чисто мнимо. Если для каждой точки v поля k показатель p в локальной степени $n_v(k)$ бесконечен, то* $\mathrm{cd}_p(G_k) \leqslant 1$.

[Поле называется „чисто мнимым", если оно не может быть погружено в $\mathbf{R}$. Это означает, что $n_v(k) = 2$ для каждой точки k, определяемой архимедовым нормированием.]

Доказательство. Прежде всего докажем, что p-примарная компонента группы $\mathrm{Br}(k)$ равна нулю. Пусть $x \in \mathrm{Br}(k)$ и $px = 0$. Так как $k = \varinjlim k_i$, то $\mathrm{Br}(k) = \varinjlim \mathrm{Br}(k_i)$ и x определяется некоторым элементом $x_0 \in \mathrm{Br}(k_{i_0})$. Однако известно (ср., например, Артин, Тэйт [1]), что всякий элемент группы Брауэра числового поля определяется своими локальными образами, которые задаются инвариантами, принадлежащими группе $\mathbf{Q}/\mathbf{Z}$ [1]).

Если $i \geqslant i_0$, то образ $x(i)$ элемента x в группе $\mathrm{Br}(k_i)$ имеет вполне определенные локальные инварианты; обозначим через W_i подмножество V_i, образованное точками, в которых локальный инвариант $x(i)$ отличен от нуля. Множества W_i образуют проективную систему (для $i \geqslant i_0$);

---

[1]) Канонические вложения $k \to k_i$ индуцируют гомоморфизм φ: $\mathrm{Br}(k) \to \prod_i \mathrm{Br}(k_i)$. Легко видеть, что $\prod$ можно заменить на $\coprod$, и из глобальной теории полей классов следует, что φ — вложение. С другой стороны, локальная теория полей классов показывает, что $\mathrm{Br}(k_i) = \mathbf{Q}/\mathbf{Z}$ (ср. далее, стр. 110). — *Прим. перев.*

покажем, что $\varprojlim W_i = \varnothing$. Действительно, если $v \in \varprojlim W_i$, то образ элемента x в каждой группе Брауэра $\mathrm{Br}((k_i)_v)$ отличен от нуля. Однако известно, что при расширении локального поля инвариант элемента группы Брауэра умножается на степень расширения (ср. [CL], стр. 201). Если теперь v — неархимедова точка, то p^∞ делит $n_v(k)$ и для достаточно большого i степень $(k_i)_v$ над $(k_{i_0})_v$ делится на p, отсюда следует, что инвариант $x(i)$ в точке v равен нулю, что противоречит сделанному предположению. Аналогично если точка v архимедова (что возможно только при $p = 2$), то для достаточно больших i поля $(k_i)_v$ совпадают с $\mathbf{C}$ и инвариант $x(i)$ в точке v снова нулевой. Итак, $\varprojlim W_i = \varnothing$, а так как W_i — конечные множества, отсюда следует, что $W_i = \varnothing$ для достаточно большого i (ср. гл. I, п. 1.4, лемма 3), откуда $x(i) = 0$ и $x = 0$. Таким образом, доказано, что $\mathrm{Br}(k)(p) = 0$.

Аналогичные рассуждения показывают, что $\mathrm{Br}(k')(p) = 0$ для любого алгебраического расширения k' поля k. Применяя предложение 4, получаем, что $\mathrm{cd}_p(G_k) \leqslant 1$, что и требовалось доказать.

Следствие. *Если поле k чисто мнимо и локальная степень каждой неархимедовой точки k равна ∞, то* $\dim(k) \leqslant 1$.

Действительно, поле k совершенно и $\mathrm{cd}_p(G_k) \leqslant 1$ для любого p, остается применить предложение 6.

Замечание. Неизвестно, обязательно ли поле k, удовлетворяющее условиям сформулированного следствия, будет полем типа (C_1).

Упражнение. Доказать утверждение, обратное предложению 9 (использовать сюръективность канонического отображения $\mathrm{Br}(k) \to \mathrm{Br}(k_v)$).

§ 4. ТЕОРЕМЫ ПЕРЕХОДА К РАСШИРЕНИЯМ

4.1. Алгебраические расширения

Предложение 10. *Пусть k' — алгебраическое расширение поля k и p — простое число. Тогда* $\mathrm{cd}_p(G_{k'}) \leqslant \mathrm{cd}_p(G_k)$, *причем равенство имеет место в следующих двух случаях:*

(i) *степень* $[k'\colon k]_s$ *взаимно проста с* p;
(ii) $\mathrm{cd}_p(G_k) < \infty$ *и* $[k'\colon k]_s < \infty$.

Группа Галуа $G_{k'}$ отождествляется с подгруппой группы Галуа G_k индекса $[k'\colon k]_s$. Утверждение следует теперь из предложения 14 гл. I.

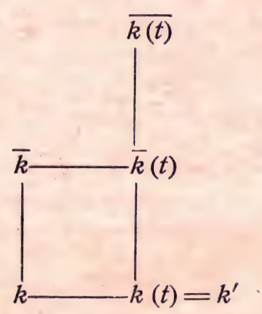
4.2. Трансцендентные расширения

Предложение 11. *Пусть k' — расширение поля k степени трансцендентности N. Для любого простого числа p*

$$\mathrm{cd}_p(G_{k'}) \leqslant N + \mathrm{cd}_p(G_k).$$

Равенство имеет место в случае, когда $\mathrm{cd}_p(G_k) < \infty$, поле k' конечного типа над k и p отлично от характеристики поля k.

В силу предложения 10 можно ограничиться случаем $k' = k(t)$, тогда $N = 1$. Пусть $\bar{k}$ обозначает алгебраическое замыкание поля k; тогда $\bar{k}$ — нормальное расширение с группой Галуа G_k, линейно-свободное с расширением $k(t)/k$. Отсюда следует, что группа Галуа расширения $\bar{k}(t)/k(t)$ отождествляется с группой G_k. С другой стороны, если H обозначает группу Галуа расширения $\overline{k(t)}/\bar{k}(t)$, то теорема Тзена показывает, что $\mathrm{cd}(H) \leqslant 1$.



Так как $G_k/H = G_k$, то искомое неравенство следует из предложения 15 гл. I.

Осталось показать, что, когда $\mathrm{cd}_p(G_k) < \infty$ и p отлично от характеристики k, имеет место равенство. Заменим G_k одной из ее силовских p-подгрупп; тогда можно

считать G_k про-p-группой, которая должна действовать на группу корней p-й степени из единицы μ_p тривиально, что показывает, что корни p-й степени из 1 принадлежат полю k.

Положим $d = \mathrm{cd}_p(G_k)$. Покажем, что $H^{d+1}(G_{k'}, \mu_p) \neq 0$, откуда будет следовать нужное нам равенство. Спектральная последовательность расширений групп (ср. гл. I, п. 3.3) показывает прежде всего, что

$$H^{d+1}(G_{k'}, \mu_p) = H^d(G_k, H^1(H, \mu_p)).$$

Однако $H^1(H, \mu_p) = H^1(\bar{k}(t), \mu_p)$. Положим для простоты записи $K = \bar{k}(t)$. Точная последовательность $0 \to \mu_p \to \to \mathbf{G}_m \xrightarrow{p} \mathbf{G}_m \to 0$, примененная к полю K, показывает, что $H^1(K, \mu_p) = K^*/K^{*p}$, и этот изоморфизм согласован с действием группы $G_k = G_{k'}/H$. Таким образом,

$$H^{d+1}(G_{k'}, \mu_p) = H^d(G_k, K^*/K^{*p}).$$

Пусть $w: K^* \to \mathbf{Z}$ — нормирование поля $K = \bar{k}(t)$, определяемое некоторым элементом поля k (например, нулем); переход к факторгруппе определяет сюръективный гомоморфизм $K^*/K^{*p} \to \mathbf{Z}/p\mathbf{Z}$, который согласован с действием группы G_k. Таким образом, имеем гомоморфизм

$$H^d(G_k, K^*/K^{*p}) \to H^d(G_k, \mathbf{Z}/p\mathbf{Z}),$$

который к тому же сюрьективен (так как $\mathrm{cd}_p(G_k) \leqslant d$). Но так как G_k — про-p-группа, $H^d(G_k, \mathbf{Z}/p\mathbf{Z}) \neq 0$. Отсюда вытекает, что $H^d(G_k, K^*/K^{*p}) \neq 0$, а следовательно, $H^{d+1}(G_k, \mu_p) \neq 0$, что и требовалось доказать.

Следствие. *Если k — поле функций от одной переменной над конечным полем или поле функций от двух переменных над алгебраически замкнутым полем, то* $\mathrm{cd}(G_k) = 2$.

(Под „полем функций от r переменных над полем k_0" понимается расширение конечного типа поля k_0 степени трансцендентности r.)

Это следует из того, что $\mathrm{cd}(G_{k_0})$ есть 1 (соответственно 0), когда k_0 конечное (соответственно алгебраически замкнутое) поле.

Замечание. Предположим, что $\mathrm{cd}_p(G_k) = \infty$. Как доказал Дж. Акс [1], в этом случае $\mathrm{cd}_p(G_{k'}) = \infty$ для любого *чисто трансцендентного* расширения k' поля k. Аналогичное замечание применимо и к предложению 12, сформулированному ниже.

4.3. Локальные поля

Предложение 12. *Пусть K — поле, полное относительно дискретного нормирования, с совершенным полем вычетов k. Для любого простого числа p*

$$\mathrm{cd}_p(G_K) \leqslant 1 + \mathrm{cd}_p(G_k).$$

Если $\mathrm{cd}_p(G_k) < \infty$ и p отлично от характеристики поля k, то в предыдущей формуле имеет место равенство.

Доказательство аналогично изложенному выше. Возьмем максимальное неразветвленное расширение K_{nr} поля K. Группа Галуа этого расширения отождествляется с группой G_k; с другой стороны, когомологическая размерность группы Галуа расширения K_s/K_{nr} не больше 1 (ср. п. 3.3, а также [CL], гл. 12). Применяя предложение 15 из гл. I, получаем $\mathrm{cd}_p(G_K) \leqslant 1 + \mathrm{cd}_p(G_k)$.

Если $d = \mathrm{cd}_p(G_k)$ конечно и p взаимно просто с характеристикой K, то все сводится, как и выше, к случаю, когда G_k — про-p-группа. Вычисляя $H^{d+1}(G_K, \mu_p)$, получаем, что

$$H^{d+1}(G_K, \mu_p) = H^d\left(G_k, K_{nr}^*/K_{nr}^{*p}\right).$$

Нормирование поля K_{nr} определяет сюръективный гомоморфизм

$$K_{nr}^*/K_{nr}^{*p} \to \mathbf{Z}/p\mathbf{Z},$$

откуда следует сюръективность гомоморфизма

$$H^d\left(G_k, K_{nr}^*/K_{nr}^{*p}\right) \to H^d(G_k, \mathbf{Z}/p\mathbf{Z}).$$

Это показывает, что $H^{d+1}(G_K, \mu_p) \neq 0$, что и требовалось доказать.

Следствие. *Если поле K является p-адическим, то* $\operatorname{cd}(G_K) = 2$.

Действительно, соответствующее поле вычетов — конечное поле, а следовательно, его размерность равна 1.

4.4. Когомологическая размерность группы Галуа поля алгебраических чисел

Предложение 13. *Пусть k — поле алгебраических чисел. Если $p \neq 2$ или поле k чисто мнимо, то* $\operatorname{cd}_p(G_k) \leqslant 2$.

Доказательство основано на следующей лемме:

Лемма 1. *Для любого простого числа p существует абелево расширение K поля $\mathbf{Q}$, группа Галуа которого изоморфна $\mathbf{Z}_p$, а локальная степень $n_v(K)$ равна p^∞ для любого нормирования v поля K.*

(Так как K — расширение Галуа поля $\mathbf{Q}$, локальная степень $n_v(K)$ точки v поля K зависит только от точки поля $\mathbf{Q}$, индуцированной точкой v; если последняя определяется простым числом l, то мы пишем $n_l(K)$ вместо $n_v(K)$.)

Обозначим сначала через $\mathbf{Q}(p)$ поле, полученное присоединением к $\mathbf{Q}$ корней из 1 степени p^α для некоторого α. Хорошо известно („неприводимость многочленов деления круга“), что группа Галуа этого расширения канонически отождествляется с группой единиц U_p поля $\mathbf{Q}_p$ [1]). Кроме того, группа разложения D_l простого числа l совпадает со всей группой U_p, если $l = p$, и с замыканием подгруппы из U_p, порожденной l, если $l \neq p$ (ср. [CL],

[1]) Пусть $\mathbf{Q}(p^m)$ обозначает расширение $\mathbf{Q}$, полученное присоединением корней p^m-й степени из 1. Известно, что группа Галуа этого расширения является подгруппой группы $(\mathbf{Z}/p^m\mathbf{Z})^*$ (Бурбаки [3*], гл. 5, § 11, п. 2, предложение 2). С другой стороны, неприводимость многочлена деления круга над полем $\mathbf{Q}$ (см., например, Ван дер Варден [1*], т. 1, § 53) показывает, что порядок расширения $\mathbf{Q}(p^m)$ совпадает с порядком группы $(\mathbf{Z}/p^m\mathbf{Z})^*$ „Переходя теперь к пределу по m“, получаем нужный нам результат. — *Прим. перев.*

стр. 85)[1]). В любом случае мы видим, что группа D_l бесконечна, откуда следует, что ее порядок делится на p^∞. Заметим теперь, что U_p есть прямое произведение конечной группы на группу $\mathbf{Z}_p$ (ср., например, [CL], стр. 220)[2]). Это разложение определяет подполе K поля $\mathbf{Q}(p)$, такое, что $G(K/\mathbf{Q}) = \mathbf{Z}_p$. Так как $[\mathbf{Q}(p):K]$ конечно, локальные степени $K/\mathbf{Q}$ должны быть равны p^∞, что завершает доказательство леммы.

Вернемся теперь к предложению 13. Пусть K — поле, обладающее свойствами, сформулированными в лемме 1, и пусть L — композит K с k. Группа Галуа L/k отождествляется с замкнутой подгруппой конечного индекса группы $G(K/\mathbf{Q})$; отсюда следует, что она сама изоморфна $\mathbf{Z}_p$. Это же рассуждение показывает, что локальные степени неархимедовых точек поля K равны p^∞. В силу предложения 9 $\mathrm{cd}_p(G_L) \leqslant 1$. Так как, с другой стороны, $\mathrm{cd}_p(\mathbf{Z}_p) \leqslant 1$, предложение 15 гл. I показывает, что $\mathrm{cd}_p(G_k) \leqslant 2$, что и требовалось доказать.

---

[1]) Действительно, пусть $K = \mathbf{Q}_l$ — поле l-адических чисел, K_n — расширение K, полученное присоединением корней n-й степени из 1. Покажем, что если $(n, l) = 1$, то $G(K_n/K) = \mathbf{Z}/n\mathbf{Z}$, а если $n = l^m$, то $G(K_n/K) = (\mathbf{Z}/n\mathbf{Z})^*$, откуда нужный результат получается переходом к пределу по степеням p.

В первом случае легко видеть, что расширение K_n/K неразветвлено, поэтому его группа Галуа канонически изоморфна группе Галуа расширения степени n поля вычетов K, которая канонически отождествляется с $\mathbf{Z}/n\mathbf{Z}$ (см. Ленг [4*], гл. 2, § 4).

Во втором случае, так как $G(K_n/K)$ содержится в $(\mathbf{Z}/n\mathbf{Z})^*$ (Бурбаки [3*], гл. 5, § 11, предложение 2), достаточно показать, что степень расширения K_n/K совпадает с числом $\varphi(n) = [(\mathbf{Z}/n\mathbf{Z})^*]$. Пусть z — корень n-й степени из единицы. Положим $u = z^{l^{m-1}}$; так как это примитивный корень l-й степени из единицы, он удовлетворяет уравнению $u^{l-1} + u^{l-2} + \ldots + 1 = 0$, т. е.

$$F(z) = z^{(l-1)l^{m-1}} + z^{(l-2)l^{m-1}} + \ldots + 1 = 0.$$

Легко видеть, что $\pi = z + 1$ будет корнем многочлена $F(1+z)$, который есть многочлен Эйзенштейна степени $\varphi(n)$. Остается воспользоваться его неприводимостью для $\mathbf{Q}_l$ (Ленг [4*], гл. 2, § 5) и заметить, что π так же, как и z, порождает K_n. — *Прим. перев.*

[2]) См. также Ленг [4*], гл. 2, § 3.

4.5. Свойство (C_r)

Это свойство аналогично свойству (C_1) из п. 3.2.

(C_r) *Каждое однородное уравнение* $f(x_1, \ldots, x_n) = 0$ *степени* d *с коэффициентами из поля* k *имеет нетривиальное решение в* k^n, *если* $n > d^r$.

Выше мы видели, что $(C_1) \Rightarrow \dim(k) \leqslant 1 \Rightarrow \mathrm{cd}(G_k) \leqslant 1$. Если $r \geqslant 2$, то *неизвестно*, влечет ли свойство (C_r) выполнение неравенства $\mathrm{cd}(G_k) \leqslant r$, однако это кажется вполне возможным.

В любом случае свойство (C_r) гарантирует выполнение условий теорем „перехода к расширениям“ аналогично тому, что доказано в п. 4.1 и 4.2. Более точно:

(а) Если k' — алгебраическое расширение поля k и поле k обладает свойством (C_r), то k' — также поле типа (C_r). (Доказательство нетрудно, ср. диссертацию Ленга [1].)

(б) Более общо, если k' — расширение поля k степени трансцендентности N и k удовлетворяет условию (C_r), то k' удовлетворяет (C_{r+N}) (ср. диссертацию Ленга [1] и дополнение Нагаты [1]).

Напротив, неизвестно, можно ли доказать утверждение, аналогичное предложению 12. Для этого нужно было бы доказать, что если K — локальное поле, поле вычетов которого удовлетворяет (C_r), то K само типа (C_{r+1}); отсюда бы следовало, например, что p-адическое поле — поле типа (C_2), что пока не доказано [1]) (известно только, что p-адическое поле удовлетворяет свойству (C_2) для однородных многочленов степени $d \leqslant 3$). Тем более неизвестно, обладает ли всякое чисто мнимое поле свойством (C_2).

Свойство (C_2) имеет некоторые следствия, полезные при изучении классических групп (которые часто можно доказать и непосредственно).

(1) Каждая квадратичная форма от 5 переменных над k представляет 0. Это позволяет полностью классифицировать квадратичные формы над k по их рангу, дискриминанту и инварианту Минковского — Хассе — Витта, ср., например, Витт [1].

---

[1]) Эта гипотеза опровергнута Òержаняном (Terjanian) сначала для $p = 2$, а затем и для всех остальных значений p. — *Прим. ред.*

(2) Если D — тело с центром k, конечное над k, то приведенная норма N_{red}: $D^* \to k^*$ сюръективна.

Это непосредственное следствие условия (C_2): если положить $n^2 = [D:k]$ и $a \in k^*$, то уравнение $N_{red}(x) = at^n$ однородно степени n от $n^2 + 1$ неизвестных; оно имеет нетривиальное решение, а это показывает, что $a \in \mathrm{Im}(N_{red})$.

В случае если каждое алгебраическое расширение k' поля k удовлетворяет условиям (1) и (2), мы говорим, что k удовлетворяет условию (C_2'). Легко показать (соответственно трудно), что p-адическое поле (соответственно чисто мнимое) удовлетворяет условию (C_2').

§ 5. *p*-АДИЧЕСКИЕ ПОЛЯ

На всем протяжении этого параграфа k обозначает *поле p-адических* чисел, т. е. некоторое конечное расширение поля $\mathbf{Q}_p$. Каждое такое поле является полным относительно дискретного нормирования v, и его поле вычетов k_0 является конечным расширением $\mathbf{F}_{p^f}$ простого поля $\mathbf{F}_p$. Поле k локально компактно.

5.1. Напоминания

(a) *Структура мультипликативной группы* k^*. Пусть $U(k)$ обозначает группу единиц поля k. Тогда имеет место точная последовательность

$$0 \to U(k) \to k^* \xrightarrow{v} \mathbf{Z} \to 0.$$

Группу $U(k)$ можно рассматривать как некоторую коммутативную компактную аналитическую группу, определенную над полем $\mathbf{Q}_p$. Ее размерность N равна степени $[k:\mathbf{Q}_p]$. Согласно теории Ли, группа $U(k)$ изоморфна произведению некоторой конечной группы F на группу $(\mathbf{Z}_p)^N$. Очевидно, что F совпадает с группой корней из единицы, содержащихся в k, в частности F — *циклическая* группа.

Из такого расщепления группы k^* следует, что для любого $n \geqslant 1$ факторгруппа k^*/k^{*n} *конечна*, и нетрудно вычислить ее порядок.

(б) *Когомологическая размерность* группы Галуа G_k алгебраического замыкания $\bar{k}/k$ равна 2 (см. п. 4. 3, следствие предложения 12).

(в) *Группа Брауэра* $\operatorname{Br}(k) = H^2(k, \mathbf{G}_m)$ *отождествляется с группой* $\mathbf{Q}/\mathbf{Z}$, см. [CL], гл. XIII. Напомним кратко, как происходит это отождествление. Обозначим через k_{nr} максимальное неразветвленное расширение поля k. Прежде всего доказывается, что $\operatorname{Br}(k) = H^2(k_{nr}/k, \mathbf{G}_m)$, иначе говоря, каждый элемент из $\operatorname{Br}(k)$ распадается над некоторым неразветвленным расширением. Далее, нормирование v задает изоморфизм $H^2(k_{nr}/k, \mathbf{G}_m) \to H^2(k_{nr}/k, \mathbf{Z})$. Так как $G(k_{nr}/k) = \hat{\mathbf{Z}}$, группа $H^2(k_{nr}/k, \mathbf{Z})$ может быть отождествлена с группой $\mathbf{Q}/\mathbf{Z}$, что дает искомый изоморфизм.

5.2. Когомологии конечных G_k-модулей

Здесь и всюду в дальнейшем через μ_n обозначается группа корней n-й степени из 1 в $\bar{k}$. Группа μ_n очевидным образом снабжена структурой G_k-модуля.

Лемма 2. *Имеют место равенства* $H^1(k, \mu_n) = k^*/k^{*n}$, $H^2(k, \mu_n) = \mathbf{Z}/n\mathbf{Z}$ и $H^i(k, \mu_n) = 0$ *для каждого* $i \geqslant 3$. *В частности, все группы* $H^i(k, \mu_n)$ *конечны.*

В точной последовательности когомологий, соответствующей точной последовательности групп (см. п. 2. 3)

$$0 \to \mu_n \to \mathbf{G}_m \to \mathbf{G}_m \to 0,$$

имеем $H^0(k, \mathbf{G}_m) = k^*$, $H^1(k, \mathbf{G}_m) = 0$ и $H^2(k, \mathbf{G}_m) = \mathbf{Q}/\mathbf{Z}$. Отсюда определяются группы $H^i(k, \mu_n)$, $i \leqslant 2$. Случай $i \geqslant 3$ тривиален, поскольку $\operatorname{cd}(G_k) = 2$.

Предложение 14. *Пусть A — конечный G_k-модуль, тогда группы $H^n(k, A)$ конечны для всех n.*

Очевидно, существует такое конечное расширение Галуа K поля k, что модуль A становится изоморфным (как G_k-модуль) некоторой прямой сумме модулей вида μ_n. В силу леммы 2 все группы $H^j(K, A)$ конечны. Из спектральной последовательности

$$H^i(G(K/k), H^j(K, A)) \Rightarrow H^n(k, A)$$

следует тогда, что группы $H^n(k, A)$ также конечны. В частности, группы $H^2(k, A)$ конечны, что позволяет на основании результатов гл. I, п. 3. 5, определить для группы G_k дуализирующий модуль I.

Теорема 1. *Дуализирующий модуль I изоморфен модулю μ, являющемуся объединением всех μ_n, $n \geqslant 1$.*

Отметим, что μ изоморфен $\mathbf{Q}/\mathbf{Z}$ как абелева группа, но не как G_k-модуль.

Для упрощения обозначений положим $G = G_k$. Пусть n — целое число, большее или равное 1, и I_n — подмодуль модуля I, порожденный элементами, которые аннулируются умножением на n. Известно, что модуль I является также дуализирующим модулем для произвольной подгруппы H группы G, а группа $\mathrm{Hom}_H(\mu_n, I_n) = \mathrm{Hom}_H(\mu_n, I)$ двойственна группе $H^2(H, \mu_n)$. В силу леммы 2 последняя группа изоморфна $\mathbf{Z}/n\mathbf{Z}$ (надо взять расширение поля k, соответствующее подгруппе H). В частности, $\mathrm{Hom}_H(\mu_n, I_n)$ *не зависит* от H; это показывает, что $\mathrm{Hom}(\mu_n, I_n) = \mathbf{Z}/n\mathbf{Z}$ действует на эту группу тривиально. Пусть $f_n\colon \mu_n \to I_n$ — элемент из $\mathrm{Hom}(\mu_n, I_n)$, соответствующий канонической образующей группы $\mathbf{Z}/n\mathbf{Z}$. Легко видеть, что f_n является *изоморфизмом группы μ_n на группу I_n*, согласованным с действием G на этих группах. Устремляя n к бесконечности (мультипликативно!), получаем изоморфизм модуля μ на модуль I, что доказывает теорему.

[Не обязательно даже проверять, что определенные выше изоморфизмы f_n продолжают друг друга, достаточно применить лемму 3 гл. I, п 1. 4, к проективной системе $\{\mathrm{Isom}(\mu_n, I_n)\}$.]

Теорема 2. *Пусть A — конечный G_k-модуль. Положим* $A' = \mathrm{Hom}(A, \mu) = \mathrm{Hom}(A, \mathbf{G}_m)$.

Тогда для каждого целого i, $0 \leqslant i \leqslant 2$, $\cup$-произведение

$$H^i(k, A) \times H^{2-i}(k, A') \to H^2(k, \mu) = \mathbf{Q}/\mathbf{Z}$$

осуществляет двойственность между конечными группами

$$H^i(k, A) \quad и \quad H^{2-i}(k, A').$$

При $i=2$ это определение дуализирующего модуля. Случай $i=0$ сводится к случаю $i=2$ заменой A на A' с учетом того, что $(A')'=A$. Из этих же соображений в случае $i=1$ достаточно доказать, что канонический гомоморфизм

$$H^1(k, A) \to H^1(k, A')^* = \mathrm{Hom}(H^1(k, A'), \mathbf{Q}/\mathbf{Z})$$

инъективен. Но это „чисто формально" следует из уже известных фактов. В самом деле, поскольку $H^1(k, A)$ — стирающий функтор, A можно вложить в некоторый G_k-модуль B так, что соответствующий гомоморфизм $H^1(k, A) \to H^1(k, B)$ будет нулевым. Полагая $C=B/A$, получаем коммутативную диаграмму

$$\begin{array}{ccccc} H^0(k, B) & \to & H^0(k, C) & \xrightarrow{\delta} & H^1(k, A) \\ \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow \\ H^2(k, B')^* & \to & H^2(k, C')^* & \to & H^1(k, A')^*. \end{array}$$

Так как α и β биективны и δ сюръективен, γ должен быть инъективным, что и требовалось доказать.

Замечания. 1. Предыдущая теорема двойственности принадлежит Тейту. В первоначальном доказательстве (воспроизведенном в заметках Ленга) Тейт вводил когомологии „торов" и существенным образом использовал теоремы Накаямы (см. [CL], гл. IX). Пуату дал другое доказательство этой теоремы, заключающееся в сведении с помощью „отвинчивания" к случаю $A=\mu_n$ (см. упражнение 1).

2. В случае когда k — поле формальных степенных рядов $k_0((T))$ над конечным полем k_0 из p^f элементов, приведенные выше результаты остаются в силе без всяких изменений, если порядок группы А *взаимно прост* с p. Для p-примарных модулей ситуация изменяется. Группу $A'=\mathrm{Hom}(A, \mathbf{G}_m)$ надо интерпретировать в этом случае как алгебраическую группу размерности нуль (соответствующая алгебра может иметь нильпотентные элементы) и брать когомологии этой группы не в смысле когомологий Галуа (которые ничего не дают), а в смысле „радикальных" когомологий. Более того, так как группа $H^1(k, A)$ не будет, вообще говоря, конечной, нужно

снабдить ее некоторой топологией и взять группу непрерывных характеров. Со всеми этими изменениями теорема двойственности сохраняется. Подробности см. в диссертации Шатца [1]).

Упражнения. 1) Применяя теорему двойственности к модулю $A = \mathbf{Z}/n\mathbf{Z}$, показать, что получается новое доказательство двойственности (известной в локальной теории полей классов) между группами $\mathrm{Hom}(G_k, \mathbf{Z}/n\mathbf{Z})$ и k^*/k^{*n}. В случае когда k содержит корни n-й степени из единицы, группу A можно отождествить с группой $A' = \mu_n$. Показать, что получаемое таким образом отображение $k^*/k^{*n} \times k^*/k^{*n} \to \mathbf{Q}/\mathbf{Z}$ задается *символом Гильберта* (см. [CL], гл. XIV).

2) Возьмем за k некоторое поле, полное относительно дискретного нормирования, поле вычетов k_0 которого является квазиконечным (см. [CL], стр. 198) [2]). Показать, что в этом случае теоремы 1 и 2 остаются в силе, если только ограничиваться конечными модулями, порядки которых взаимно просты с характеристикой поля k_0.

3) „Чисто формальная" часть доказательства теоремы 2 является на самом деле некоторой теоремой о морфизмах когомологических функторов. Что это за теорема?

4) Показать непосредственно с использованием критерия Вердье (см. гл. IV, стр. 195), что G_k является строгой группой Коэна—Маколея. Вывести отсюда другое доказательство теоремы 2.

5.3. Первые приложения

Предложение 15. *Строгая когомологическая размерность группы G_k равна 2.*

Действительно, группа $H^0(G_k, I) = H^0(G_k, \mu)$ совпадает с группой всех корней из единицы, содержащихся в k. Следовательно, в силу п. 5.1 она конечна. В таком случае предложение вытекает из предложения 19 гл. I.

---

[1]) См. Шатц [1]. — *Прим. перев.*

[2]) Поле k называется квазиконечным, если оно совершенно и группа Галуа его алгебраического замыкания $G(\bar{k}/k)$ изоморфна свободной проконечной группе $\hat{\mathbf{Z}}$. — *Прим. перев.*

Предложение 16. *Для всякого абелева многообразия A, определенного над k, имеет место равенство $H^2(k, A) = 0$.*

Для каждого $n \geqslant 1$ обозначим через A_n подгруппу группы A, являющуюся ядром гомоморфизма умножения на n. Непосредственно видно, что $H^2(k, A) = \varinjlim H^2(k, A_n)$. Согласно теореме двойственности, группа $H^2(k, A_n)$ двойственна группе $H^0(k, A'_n)$. С другой стороны, если обозначить через B абелево многообразие, *двойственное* к A (в смысле двойственности абелевых многообразий), то известно, что группу A'_n можно отождествить с группой B_n. Все сводится, таким образом, к доказательству того, что

$$\varprojlim H^0(k, B_n) = 0.$$

Но $B(k) = H^0(k, B)$ — абелева компактная p-адическая группа Ли. Следовательно, ее периодическая подгруппа конечна. Таким образом, все $H^0(k, B_n)$ содержатся в фиксированной конечной подгруппе группы B, откуда легко следует обращение в нуль группы $\varprojlim H^0(k, B_n)$.

Замечание. Тейт доказал, что группу $H^1(k, A)$ можно отождествить с группой, двойственной компактной группе $H^0(k, B)$. Не похоже, что этот результат следует просто из теоремы двойственности, доказанной в предыдущем пункте.

Упражнение. Пусть T — некоторый тор, определенный над k. Показать, что следующие условия эквивалентны:

(i) группа $T(k)$ компактна;
(ii) всякий k-гомоморфизм T в $\mathbf{G}_m$ тривиален;
(iii) $H^2(k, T) = 0$.

5.4. Характеристика Эйлера — Пуанкаре (элементарный случай)

Пусть A — конечный G_k-модуль и $h^i(A)$ — порядки конечных групп $H^i(G_k, A)$. Положим

$$\chi(A) = \frac{h^0(A) \cdot h^2(A)}{h^1(A)}.$$

Получим некоторое рациональное число, большее 0, которое называется *характеристикой Эйлера — Пуанкаре модуля* A. Пусть $0 \to A \to B \to C \to 0$ — точная последовательность G_k-модулей. Тогда легко видеть, что

$$\chi(B) = \chi(A) \cdot \chi(C).$$

Это „аддитивность“ характеристики Эйлера — Пуанкаре. Тейт показал, что $\chi(A)$ зависит только от *порядка* a группы A (вернее, он установил, что $\chi(A) = 1/(\mathfrak{o}: a\mathfrak{o})$, где $\mathfrak{o}$ обозначает кольцо целых элементов из k). Мы ограничимся пока одним элементарным частным случаем.

Предложение 17. *Если порядок группы* A *взаимно прост с* p, *то* $\chi(A) = 1$.

Воспользуемся спектральной последовательностью, ассоциированной с башней расширений $k \to k_{nr} \to \bar{k}$. Известно, что группа Галуа $G(k_{nr}/k)$ изоморфна $\hat{\mathbf{Z}}$. Обозначим через U группу Галуа $G(\bar{k}/k_{nr})$. Из теории групп ветвлений следует, что силовская p-подгруппа U_p группы U является нормальным делителем и факторгруппа U/U_p изоморфна прямому произведению групп $\mathbf{Z}_l$, $l \neq p$. Отсюда легко выводится, что группы $H^i(U, A)$ конечны для всех i и обращаются в нуль при $i \geqslant 2$. Спектральная последовательность

$$H^i(k_{nr}/k, H^j(k_{nr}, A)) \Rightarrow H^n(k, A)$$

в таком случае имеет вид

$$H^i(\hat{\mathbf{Z}}, H^j(U, A)) \Rightarrow H^n(k, A).$$

Из нее следует, что

$$H^0(k, A) = H^0(\hat{\mathbf{Z}}, H^0(U, A)), \; H^2(k, A) = H^1(\hat{\mathbf{Z}}, H^1(U, A))$$

и имеет место точная последовательность

$$0 \to H^1(\hat{\mathbf{Z}}, H^0(U, A)) \to H^1(k, A) \to H^0(\hat{\mathbf{Z}}, H^1(U, A)) \to 0,$$

Воспользуемся теперь легко проверяемым фактом, что для всякого конечного $\hat{\mathbf{Z}}$-модуля M группы $H^0(\hat{\mathbf{Z}}, M)$ и $H^1(\mathbf{Z}, M)$ имеют одинаковое число элементов. Применяя

8*

это к группам

$$M = H^0(U, A) \quad \text{и} \quad M = H^1(U, A),$$

получаем, что $h^1(A) = h^0(A) \cdot h^2(A)$, откуда $\chi(A) = 1$.

Упражнение. Показать, что группа U_p, определенная в ходе доказательства предложения 17, является свободной про-p-группой. Из этого следует, что для всякого периодического G_k-модуля A имеет место равенство $H^j(U, A) = 0$ при $j \geqslant 2$. Показать, что если A — ненулевая p-группа, то группа $H^1(U, A)$ уже *не является конечной*.

5.5. Неразветвленные когомологии

Сохраним обозначения предыдущего пункта. G_k-модуль A будем называть *неразветвленным*, если группа $U = G(\bar{k}/k_{nr})$ действует *тривиально* на A. Так как $G(k_{nr}/k) = \hat{\mathbf{Z}}$, то это позволяет рассматривать A как $\hat{\mathbf{Z}}$-модуль. В частности, определены группы когомологий $H^i(k_{nr}/k, A)$. Мы будем обозначать эти группы через $H^i_{nr}(k, A)$.

Предложение 18. *Пусть A — конечный неразветвленный G_k-модуль. Тогда*

(а) $H^0_{nr}(k, A) = H^0(k, A)$;

(б) *группа $H^1_{nr}(k, A)$ отождествляется с подгруппой группы $H^1(k, A)$ и порядок ее равен порядку группы $H^0(k, A)$;*

(в) $H^i_{nr}(k, A) = 0$ *при* $i \geqslant 2$.

Утверждение (а) тривиально. Утверждение (б) следует из того, что группы $H^0(\hat{\mathbf{Z}}, A)$ и $H^1(\hat{\mathbf{Z}}, A)$ имеют одинаковое число элементов. Утверждение (в) следует из того, что когомологическая размерность $\hat{\mathbf{Z}}$ равна 1.

Предложение 19. *Пусть A — конечный неразветвленный G_k-модуль, порядок которого взаимно прост с p. Тогда модуль $A' = \mathrm{Hom}(A, \mu)$ обладает этими же свойствами. Более того, в двойственности между $H^1(k, A)$ и $H^1(k, A')$ подгруппы $H^1_{nr}(k, A)$ и $H^1_{nr}(k, A')$ являются ортогональными дополнениями друг к другу.*

Пусть $\overline{\mu}$ — подгруппа группы μ, порожденная элементами, порядки которых взаимно просты с p. Хорошо известно, что $\overline{\mu}$ является неразветвленным G_k-модулем (каноническая образующая F группы $G(k_{nr}/k) = \hat{\mathbf{Z}}$ действует на $\overline{\mu}$ по формуле $\lambda \to \lambda^q$, где q — число элементов поля вычетов k_0). Так как $A' = \operatorname{Hom}(A, \overline{\mu})$, из этого тотчас же следует неразветвленность модуля A'.

Ясно, что $\cup$-произведение $H^1_{nr}(k, A) \times H^1_{nr}(k, A') \to \to H^2(k, \mu)$ пропускается через группу $H^2_{nr}(k, \overline{\mu})$, которая равна нулю. Отсюда следует, что группы $H^1_{nr}(k, A)$ и $H^1_{nr}(k, A')$ ортогональны. Чтобы доказать, что каждая из них является ортогональным дополнением к другой, достаточно проверить, что порядок $h^1(A)$ группы $H^1(k, A)$ равен произведению $h^1_{nr}(A) \cdot h^1_{nr}(A')$ порядков групп $H^1_{nr}(k, A)$ и $H^1_{nr}(k, A')$. Но из предложения 18 следует, что $h^1_{nr}(A) = h^0(A)$ и аналогично $h^1_{nr}(A') = h^0(A')$. В силу теоремы двойственности $h^0(A') = h^2(A)$. Далее из того, что $\chi(A) = 1$ (см. предложение 17), получаем $h^1(A) = h^0(A) \cdot h^2(A) = h^1_{nr}(A) \cdot h^1_{nr}(A')$, что и требовалось доказать.

Упражнение. Распространить предложения 17, 18, 19 на полные относительно дискретного нормирования поля с квазиконечными полями вычетов. Можно ли сделать то же самое с предложениями 15 и 16?

5.6. Группа Галуа максимального p-расширения поля k

Пусть $k(p)$ — максимальное p-расширение поля k в смысле § 2. По определению группа Галуа $G_k(p)$ расширения $k(p)/k$ есть наибольшая факторгруппа группы G_k, являющаяся про-p-группой.

Изучим структуру этой группы.

Предложение 20. *Пусть A — p-примарный периодический G_k-модуль. Тогда для всякого целого числа $i \geqslant 0$ канонический гомоморфизм*

$$H^i(G_k(p), A) \to H^i(G_k, A)$$

является изоморфизмом.

Воспользуемся следующей леммой:

Лемма 3. *Пусть K — алгебраическое расширение поля k, степень которого делится на p^∞. Тогда* $\mathrm{Br}(K)(p)=0$.

Представим K в виде объединения конечных подрасширений K_α. Тогда $\mathrm{Br}(K)=\varinjlim \mathrm{Br}(K_\alpha)$. Кроме того, каждая группа $\mathrm{Br}(K_\alpha)$ изоморфна группе $\mathbf{Q}/\mathbf{Z}$, и если K_β содержит K_α, то соответствующий гомоморфизм $\mathrm{Br}(K_\alpha)$ в $\mathrm{Br}(K_\beta)$ является просто умножением на степень $[K_\beta: K_\alpha]$ (см. [CL], стр. 201). Отсюда легко следует утверждение леммы (ср. доказательство предложения 9, п. 3.3).

Возвратимся к доказательству предложения 20. Поле $k(p)$ содержит максимальное неразветвленное p-расширение поля k, группа Галуа которого изоморфна $\mathbf{Z}_p$ и, следовательно, $[k(p):k]=p^\infty$. Условие леммы 3 выполнено, таким образом, для каждого алгебраического расширения K поля $k(p)$. Отсюда заключаем, что если $I=G(\bar{k}/k(p))$ — группа Галуа замыкания поля $k(p)$, то $\mathrm{cd}_p(I)\leqslant 1$, см. п. 2.3, предложение 4. Следовательно, $H^i(I, A)=0$ для всех $i\geqslant 2$. Но группа $H^1(I, A)$ также равна нулю, поскольку любой гомоморфизм группы I в p-группу A тривиален (см. п. 2.1, доказательство предложения 2). Спектральная последовательность расширений групп показывает теперь, что все гомоморфизмы

$$H^i(G_k/I,\ A)\to H^i(G_k,\ A)$$

являются изоморфизмами, что и требовалось доказать.

Теорема 3. *Если поле k не содержит первообразных корней p-й степени из единицы, то группа $G_k(p)$ является свободной про-p-группой ранга $N+1$, где $N=[k:\mathbf{Q}_p]$.*

В силу предложения 20 имеет место равенство $H^2(G_k(p), \mathbf{Z}/p\mathbf{Z})=H^2(k, \mathbf{Z}/p\mathbf{Z})$. По теореме двойственности последняя группа двойственна группе $H^0(k, \mu_p)$, которая по условию теоремы равна нулю. Следовательно, $H^2(G_k(p), \mathbf{Z}/p\mathbf{Z})=0$. Это показывает, что группа $G_k(p)$ свободна, см. гл. I, п. 4.2. Для вычисления ее ранга достаточно вычислить размерность группы $H^1(G_k(p), \mathbf{Z}/p\mathbf{Z})$, которая изоморфна группе $H^1(G_k, \mathbf{Z}/p\mathbf{Z})$. Согласно локальной теории полей классов (или по теореме двойственности), группа $H^1(G_k, \mathbf{Z}/p\mathbf{Z})$ двойственная группе k^*/k^{*p}, которая в силу упоминаемых

в п. 5.1 результатов является векторным $\mathbf{F}_p$-пространством размерности $N+1$. Теорема доказана.

Теорема 4. *Если поле k содержит первообразные корни p-й степени из единицы, то группа $G_k(p)$ является про-p-группой Пуанкаре размерности 2 и имеет ранг $N+2$, где $N=[k:\mathbf{Q}_p]$. Дуализирующим модулем для нее является p-примарная компонента $\mu(p)$ группы корней из единицы μ.*

По условию имеем $H^0(k, \mu_p)=\mathbf{Z}/p\mathbf{Z}$, откуда $H^2(k, \mathbf{Z}/p\mathbf{Z})=\mathbf{Z}/p\mathbf{Z}$. Применяя предложение 20, получаем, что

$$H^2(G_k(p), \mathbf{Z}/p\mathbf{Z})=\mathbf{Z}/p\mathbf{Z} \text{ и } H^i(G_k(p), \mathbf{Z}/p\mathbf{Z})=0 \text{ при } i>2.$$

Отсюда уже следует, что $\mathrm{cd}_p(G_k(p))=2$. Для доказательства того, что $G_k(p)$ есть группа Пуанкаре, осталось проверить, что $\cup$-произведение

$$H^1(G_k(p), \mathbf{Z}/p\mathbf{Z})\times H^1(G_k(p), \mathbf{Z}/p\mathbf{Z})\to$$
$$\to H^2(G_k(p), \mathbf{Z}/p\mathbf{Z})=\mathbf{Z}/p\mathbf{Z}$$

является невырожденной билинейной формой. Но это легко следует из предложения 20 и из аналогичного факта для когомологий поля k (нужно заметить, что группы μ_p и $\mathbf{Z}/p\mathbf{Z}$ изоморфны).

Ранг группы $G_k(p)$ равен размерности $H^1(G_k(p), \mathbf{Z}/p\mathbf{Z})$ или размерности $\mathbf{F}_p$-пространства k^*/k^{*p}, т. е. $N+2$.

Осталось доказать, что $\mu(p)$ является дуализирующим модулем для $G_k(p)$. Для этого заметим прежде всего, что так как поле k содержит группу μ_p, то поле, полученное присоединением к k корней p^n-й степени из единицы, является абелевым расширением степени, не превосходящей p^{n-1}, и содержится, следовательно, в поле $k(p)$. Отсюда следует, что $\mu(p)$ является $G_k(p)$-модулем и в силу предложения 20

$$H^2(G_k(p), \mu(p))=H^2(k, \mu(p))=(\mathbf{Q}/\mathbf{Z})(p)=\mathbf{Q}_p/\mathbf{Z}_p.$$

Пусть теперь A — некоторый конечный p-примарный $G_k(p)$-модуль. Положим

$$A'=\mathrm{Hom}(A, \mu)=\mathrm{Hom}(A, \mu(p)).$$

Группа A' также является $G_k(p)$-модулем. Если $0 \leqslant i \leqslant 2$, то $\cup$-произведение определяет некоторое билинейное отображение

$$H^i(G_k(p), A) \times H^{2-i}(G_k(p), A') \to$$
$$\to H^2(G_k(p), \mu(p)) = \mathbf{Q}_p/\mathbf{Z}_p.$$

Предложение 20 показывает, что это отображение совпадает с соответствующим отображением для когомологий всей группы G_k и, согласно теореме 2, является, следовательно, двойственностью между группами $H^i(G_k(p), A)$ и $H^{2-i}(G_k(p), A')$. Таким образом, $\mu(p)$ — дуализирующий модуль для $G_k(p)$. Теорема доказана.

Следствие (Кавада). *Группу $G_k(p)$ можно задать $N+2$ образующими и одним соотношением.*

Это вытекает из равенств

$$\dim H^1(G_k(p), \mathbf{Z}/p\mathbf{Z}) = N+2$$

и

$$\dim H^2(G_k(p), \mathbf{Z}/p\mathbf{Z}) = 1.$$

Замечание. В действительности структура группы $G_k(p)$ была полностью (за одним исключением) изучена Дёмушкиным. Он получил следующий результат: обозначим через p^s наибольшую степень числа p, такую, что поле k содержит корни этой степени из 1. *Предположим, что* $p^s \neq 2$ (при $p \neq 2$ это всегда так). Тогда в группе $G_k(p)$ можно выбрать образующие $x_1, \ldots, x_{N+2}$, так что единственное соотношение r между ними имеет вид

$$r = x_1^{p^s}(x_1, x_2) \ldots (x_{N+1}, x_{N+2}).$$

[Здесь (x, y) обозначает $xyx^{-1}y^{-1}$. Отметим, что из предположения $p^s \neq 2$ следует, что N четно.]

При $p=2$, $s=1$ к настоящему времени разобран только случай *нечетного* N[1]). Соотношение r записывается здесь в виде

$$r = x_1^2 x_2^4 (x_2, x_3) \ldots (x_{N+1}, x_{N+2}).$$

---

[1]) Случай четного N изучен в работах Дёмушкина [2*] и Лабюта [1*]. — *Прим. ред.*

В частности, если $k=\mathbf{Q}_2$, то группа $G_k(2)$ порождена тремя элементами x, y, z, связанными соотношением

$$x^2y^4(y, z)=1.$$

За подробностями отсылаем к заметке Дёмушкина [1], а также к докладу 252 в семинарах Бурбаки (Серр [3]).

Упражнения. 1) Пусть k_0 — совершенное поле характеристики p и $\mathfrak{g}$ — группа Галуа $\overline{k_0}$ над k_0. Обозначим через $(\mu_n)_0$ группу корней n-й степени из единицы, $(n, p)=1$, содержащихся в $\overline{k}_0$, и через $T(k_0)$ — проективный предел групп $(\mu_n)_0$. Показать, что группа $T(k_0)$ изоморфна (не канонически) прямому произведению $\hat{\mathbf{Z}}'$ групп $\mathbf{Z}_l$, $l\neq p$. Группа $\mathfrak{g}$ непрерывно действует на $T(k_0)$.

Пусть k — полное дискретно нормированное поле с полем вычетов k_0. Конечное расширение Галуа k' поля k называется *слабо разветвленным*, если порядок соответствующей группы инерции взаимно прост с p (это равносильно утверждению, что группа высшего ветвления тривиальна, см. [CL], гл. IV). Пусть K — композит всех таких расширений. Показать, что группа Галуа $G(K/k)$ изоморфна полупрямому произведению группы $\mathfrak{g}$ на группу $T(k_0)$.

Применяя этот результат к случаю $k_0=\mathbf{F}_q$, показать, что группа $G(K/k)$ изоморфна полупрямому произведению $\hat{\mathbf{Z}}$ на $\hat{\mathbf{Z}}'$ с действием вида $\lambda\to\lambda^q$. Установить, что это полупрямое произведение изоморфно проконечной группе, ассоциированной с дискретной группой, определенной двумя образующими x, y и одним соотношением $yxy^{-1}=x^q$.

2) Обозначим через k полное относительно дискретного нормирования поле с полем вычетов $\mathbf{F}_q$, где $q=p^f$. Пусть l — простое число, отличное от p. Предлагается определить структуру группы $G_k(l)$.

(a) Предположим, что $\mathbf{F}_q$ не содержит первообразного корня l-й степени из единицы, иначе говоря, $q-1$ не делится на l. Показать, что группа $G_k(l)$ изоморфна в таком случае свободной про-l-группе ранга 1 и расширение $k(l)/k$ не разветвлено.

(б) Предположим, что $q \equiv 1 \pmod{l}$. Показать, что группа $G_k(l)$ является тогда про-l-группой Пуанкаре размерности 2 и ранга 2. Используя упражнение 1, установить, что группа $G_k(l)$ может быть задана двумя образующими x, y, связанными соотношением $yxy^{-1} = x^q$. Показать, что эта группа изоморфна подгруппе аффинной группы $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, порожденной матрицами, у которых $b \in \mathbf{Z}_l$ и элемент a из $\mathbf{Z}_l^*$ является некоторой целой l-адической степенью числа q.

(в) Сохраним те же предположения, что и в пункте (б), и через m обозначим l-адическую норму числа $q-1$. Показать, что m есть наибольшее целое число среди тех, для которых k содержит корень степени l^m из единицы. Если $l \neq 2$ или если $l = 2$ и $m \neq 1$, то группа $G_k(l)$ может быть задана двумя образующими x и y и одним соотношением $yxy^{-1} = x^{1+l^m}$. Пусть $l = 2$, $m = 1$ и n равно 2-адической норме числа $q+1$. Показать, что $G_k(2)$ можно задать двумя образующими x и y, связанными соотношением $yxy^{-1} = x^{-(1+2^n)}$.

(г) Определить дуализирующий модуль для $G_k(l)$ в случае (б).

5.7. Характеристика Эйлера — Пуанкаре

Вернемся к обозначениям п. 5.4. В частности, $\mathfrak{o}$ обозначает кольцо целых элементов поля k. Обозначим далее через $\|x\|_k$ абсолютное значение элемента $x \in k$, см. [CL], стр. 37 [1]). Для каждого $x \in \mathfrak{o}$

$$\|x\|_k = \frac{1}{(\mathfrak{o} : x\mathfrak{o})}.$$

В частности,

$$\|p\|_k = p^{-N}, \quad \text{где} \quad N = [k : \mathbf{Q}_p].$$

Для всякого конечного G_k-модуля A обозначим через $\chi(k, A)$ (или просто через $\chi(A)$, если нет опасности пе-

[1]) Пусть k — локальное поле, q — число элементов его поля вычетов. Абсолютное значение $\|x\|$ элемента $x \in k$ определяется равенством $\|x\| = q^{-v(x)}$, где $v(x)$ — норма x. Абсолютное значение определяет на k некоторую ультраметрику. — *Прим. перев.*

репутать k) *характеристику Эйлера — Пуанкаре* модуля A (п. 5.4). Теорема Тейта может быть сформулирована тогда так:

Теорема 5. *Если порядок конечного G_k-модуля A равен a, то имеет место соотношение*

$$\chi(A) = \| a \|_k.$$

Оба члена этой формулы „аддитивны" по A. Поэтому, пользуясь „отвинчиванием", доказательство можно свести к случаю, когда A представляет собой векторное пространство над простым полем. В случае когда характеристика этого поля отлична от p, теорема уже была доказана ранее (предложение 17). Можно считать, таким образом, что A — *векторное пространство над* $\mathbf{F}_p$.

Кроме того, A можно рассматривать как $\mathbf{F}_p[G]$-*модуль*, где G — некоторая конечная факторгруппа группы G_k. Пусть $K(G)$ — *группа Гротендика* в категории $\mathbf{F}_p[G]$-модулей конечного типа (см., например, Джорджутти [1] или Суон [2])[1]). Функции $\chi(A)$ и $\| a \|_k$ определяют гомоморфизмы χ и φ группы $K(G)$ в $\mathbf{Q}^{+^*}$ и, следовательно, *надо доказать, что* $\chi = \varphi$. Так как $\mathbf{Q}^{+^*}$ — абелева группа без кручения, то *достаточно показать*, что χ и φ принимают одинаковые значения на элементах $x_i \in K(G)$, порождающих группу $K(G) \otimes \mathbf{Q}$. Для этого воспользуемся следующей леммой:

Лемма 4. *Для каждой подгруппы C в G обозначим через M_G^C гомоморфизм группы $K(C) \otimes \mathbf{Q}$ в группу $K(G) \otimes \mathbf{Q}$, определяемый функтором M_G^C* (см. гл. I, п. 2.5, „дуализирующий модуль"). *Тогда группа $K(G) \otimes \mathbf{Q}$ порождается образами гомоморфизмов M_G^C, где C пробегает множество циклических подгрупп в G, порядок которых взаимно прост с p.*

---

[1]) Пусть $\mathscr{C}$ — некоторая абелева категория. *Группа Гротендика* $K(\mathscr{C})$ — это абелева группа, решающая универсальную задачу в классе всех „аддитивных" отображений $\mathscr{C}$ в абелевы группы, т. е. отображений $f: \mathscr{C} \to A$, где A — абелева группа, удовлетворяющих условию $f(X) = f(Y) + f(Z)$, если X, Y, Z связаны точной последовательностью $0 \to Y \to X \to Z \to 0$. — *Прим. перев.*

Этот результат можно вывести из описания группы $K(\bar{G})\otimes \mathbf{Q}$ с помощью „модулярных характеров“. Еще проще его можно получить из общих результатов Суона (см. Суон [1]).

На основании этой леммы достаточно доказать равенство $\chi(A)=\|a\|_k$ в случае, когда A является $\mathbf{F}_p[G]$-модулем вида $M_G^C(B)$, где C — циклическая подгруппа групп G, порядок которой взаимно прост с p. Но если K — расширение поля k, соответствующее группе C, и $b=\mathrm{Card}(B)$, то

$$\chi(K,\ B)=\chi(k,\ A) \quad \text{и} \quad \|b\|_K=(\|b\|_k)^{[K:k]}=\|a\|_k.$$

Доказываемая формула эквивалентна, следовательно, формуле $\chi(K,\ B)=\|B\|_K$. Таким образом, *доказательство можно свести* (изменив основное поле) *к случаю, когда G — циклическая группа порядка, взаимно простого с p*. Это упрощает дело, поскольку алгебра $\mathbf{F}_p[G]$ является теперь *полупростой*.

Пусть L — расширение поля k, группа Галуа которого равна G. Так как порядок группы G взаимно прост с p, то

$$H^i(k,\ A)=H^0(G,\ H^i(L,\ A))$$

при всех i.

Это наводит на мысль ввести элемент $h_L(A)$ в группе $K(G)$, определенный формулой

$$h_L(A)=\sum_{i=0}^{i=2}(-1)^i\,[H^i(L,\ A)],$$

где $[H^i(L,\ A)]$ обозначает класс $\mathbf{F}_p[G]$-модуля $H^i(L,\ A)$ в $K(G)$.

Пусть, с другой стороны, θ: $K(G)\to\mathbf{Z}$ — однозначно определенный гомоморфизм группы $K(G)$ в $\mathbf{Z}$, задаваемый формулой $\theta([E])=\dim H^0(G,\ E)$ для любого $\mathbf{F}_p[G]$-модуля E. Очевидно,

$$\log_p\chi(A)=\theta(h_L(A)).$$

Но элемент $h_L(A)$ может быть явно вычислен.

Лемма 5. *Пусть $r_G\in K(G)$ — класс модуля* $\mathbf{F}_p[G]$ (*„регулярного представления“*), $N=[k:Q_p]$ *и* $d=\dim(A)$.

Тогда имеет место равенство

$$h_L(A) = -dN \cdot r_G.$$

Будем считать сначала, что лемма доказана. Тогда, поскольку $\theta(r_G) = 1$, получаем, что $\theta(h_L(A)) = -dN$, откуда

$$\chi(A) = p^{-dN} = \| p^d \|_k = \| a \|_k.$$

Осталось, следовательно, доказать лемму 5. Заметим прежде всего, что $\cup$-произведение определяет изоморфизм G-модулей

$$H^i(L, \mathbf{Z}/p\mathbf{Z}) \otimes A \to H^i(L, A).$$

Следовательно, в кольце $K(G)$

$$h_L(A) = h(L, \mathbf{Z}/p\mathbf{Z}) \cdot [A],$$

и все сводится к доказательству равенства $h_L(\mathbf{Z}/p\mathbf{Z}) = -N \cdot r_G$ (в самом деле, легко проверить, что $r_G \cdot [A] = \dim(A) \cdot r_G$). *Таким образом, можно ограничиться доказательством леммы* 5 *для* $A = \mathbf{Z}/p\mathbf{Z}$. В этом случае

$H^0(L, \mathbf{Z}/p\mathbf{Z}) = \mathbf{Z}/p\mathbf{Z}$;

$H^1(L, \mathbf{Z}/p\mathbf{Z}) = \mathrm{Hom}(G_L, \mathbf{Z}/p\mathbf{Z})$ — группа, двойственная группе L^*/L^{*p} (теория полей классов);

$H^2(L, \mathbf{Z}/p\mathbf{Z})$ — группа, двойственная группе $H^0(L, \mu_p)$ (теорема двойственности).

Пусть U обозначает группу единиц поля L. Тогда имеет место точная последовательность

$$0 \to U/U^p \to L^*/L^{*p} \to \mathbf{Z}/p\mathbf{Z} \to 0.$$

Обозначая через $h_L(\mathbf{Z}/p\mathbf{Z})^*$ элемент в $K(G)$, двойственный к $h_L(\mathbf{Z}/p\mathbf{Z})$, получаем

$$h_L(\mathbf{Z}/p\mathbf{Z})^* = -[U/U^p] + [H^0(L, \mu_p)].$$

Пусть V — подгруппа группы U, состоящая из элементов, сравнимых с 1 по модулю максимального идеала кольца $\mathfrak{o}_L$. Тогда $V/V^p = U/U^p$ и группа $H^0(L, \mu_p)$ есть не что иное как подгруппа ${}_pV$ в V, порожденная элементами $x \in V$, для которых $x^p = 1$.

В таком случае мы можем написать

$$- h_L(\mathbf{Z}/p\mathbf{Z})^* = [V/V^p] - [{}_pV] =$$
$$= [\mathrm{Tor}_0(V, \mathbf{Z}/p\mathbf{Z})] - [\mathrm{Tor}_1(V, \mathbf{Z}/p\mathbf{Z})].$$

Так как V является $\mathbf{Z}_p$-модулем конечного типа, то, как известно (это элементарные результаты теории Брауэра, см., например, диссертацию Джорджутти), выражение $[\mathrm{Tor}_0(V, \mathbf{Z}/p\mathbf{Z})] - [\mathrm{Tor}_1(V, \mathbf{Z}/p\mathbf{Z})]$ зависит только от *тензорного произведения* V на $\mathbf{Q}_p$ (или, если угодно, от *алгебры Ли* p-адической аналитической группы V). Но теорема о нормальном базисе показывает, что эта алгебра Ли является свободным $\mathbf{Q}_p[G]$-модулем ранга N. Следовательно,

$$[\mathrm{Tor}_0(V, \mathbf{Z}/p\mathbf{Z})] - [\mathrm{Tor}_1(V, \mathbf{Z}/p\mathbf{Z})] = N \cdot r_G,$$

и так как $(r_G)^* = r_G$, то $h_L(\mathbf{Z}/p\mathbf{Z}) = - N \cdot r_G$, что завершает доказательство леммы, а вместе с ней и теоремы.

Замечание. Первоначальное доказательство Тейта (воспроизведенное в заметках Ленга) не использует леммы 4, а основывается на менее точных рассуждениях „отвинчивания“. А именно оно сводится к случаю слабо разветвленного расширения Галуа L/k, но степени, возможно, делящейся на p. Изучение расширения L^*/L^{*p} становится в таком случае явно более тонкой задачей, и Тейт использует здесь один результат Ивасавы ([2], стр. 459). Впрочем, недавно он сообщил мне „когомологическое“ доказательство этого результата.

Упражнения. 1) Доказать непосредственно, что если V и V' являются $\mathbf{Z}_p[G]$-модулями конечного типа и $V \otimes \mathbf{Q}_p = V' \otimes \mathbf{Q}_p$, то

$$[V/pV] - [{}_pV] = [V'/pV'] - [{}_pV'] \text{ в } K(G).$$

[Свести к случаю, когда $V \supset V' \supset pV$, и воспользоваться точной последовательностью

$$0 \to {}_pV' \to {}_pV \to V/V' \to V'/pV' \to V/pV \to V/V' \to 0.]$$

2) Пусть F — поле характеристики p и A — конечномерное векторное пространство над F. Предположим, что группа Галуа G_k действует непрерывно (и линейно) на A;

группы когомологий $H^i(k, A)$ являются тогда векторными пространствами над F. Положим

$$\rho(A) = \sum (-1)^i \dim H^i(k, A).$$

Показать, что $\rho(A) = -N \cdot \dim(A)$, где $N = [k : \mathbf{Q}_p]$.

[Доказательство такое же, как и доказательство теоремы 5 с заменой поля $\mathbf{F}_p$ на поле F.]

3) Сохраняя предположения предыдущего упражнения, рассмотрим конечное расширение Галуа L/k с группой Галуа G, такое, что группа G_L действует тривиально на A (т. е. является $F[G]$-модулем). В группе Гротендика $F(G)$-модулей конечного типа $K_F(G)$ положим

$$h_L(A) = \sum (-1)^i [H^i(L, A)].$$

Показать, что по-прежнему имеет место формула

$$h_L(A) = -N \cdot \dim(A) \cdot r_G.$$

[Использовать теорию модулярных характеров с целью свести доказательство к случаю циклической группы G порядка, взаимно простого с p.]

4) В условиях и обозначениях предыдущих двух упражнений предположим, кроме того, что характеристика F не равна p. Показать, что тогда $\varphi(A) = 0$ и $h_L(A) = 0$ для всех A.

5.8. Группы мультипликативного типа

Пусть A — некоторый G_k-модуль *конечного типа* над $\mathbf{Z}$. Определим *двойственный* ему модуль A' следующей обычной формулой:

$$A' = \operatorname{Hom}(A, \mathbf{G}_m).$$

Группа A' представляет собой группу $\bar{k}$-точек некоторой алгебраической коммутативной группы, определенной над полем k (мы будем обозначать ее также через $\operatorname{Hom}(A, \mathbf{G}_m)$). В случае когда модуль A конечен, модуль A' также конечен. Если A свободен над $\mathbf{Z}$, то A' является *тором* с группой характеров A (см. гл. III, п. 2.1). Мы хотим распространить теорему двойственности п. 5.2 на пару (A, A').

Для каждого $i = 0, 1, 2$ $\cup$-произведение определяет билинейное отображение

$$\theta_i\colon H^i(k, A) \times H^{2-i}(k, A') \to H^2(k, \mathbf{G}_m) = \mathbf{Q}/\mathbf{Z}.$$

ТЕОРЕМА 6. (а) *Пусть* $\widehat{H^0(k, A)}$ — *пополнение абелевой группы* $H^0(k, A)$ *в топологии, определенной подгруппами конечного индекса. Тогда отображение* θ_0 *осуществляет двойственность между компактной группой* $\widehat{H^0(k, A)}$ *и дискретной группой* $H^2(k, A')$.

(б) *Отображение* θ_1 *осуществляет двойственность между конечными группами* $H^1(k, A)$ и $H^1(k, A')$.

(в) *Группу* $H^0(k, A')$ *можно канонически снабдить структурой p-адической аналитической группы. Обозначим через* $\widehat{H^0(k, A')}$ *ее пополнение в топологии, определенной открытыми подгруппами конечного индекса. Тогда отображение* θ_2 *осуществляет двойственность между дискретной группой* $H^0(k, A)$ *и компактной группой* $\widehat{H^0(k, A')}$.

[В случае когда модуль A конечен, операции пополнения в пунктах (а) и (в) можно опустить. Получается снова известная теорема 2 п. 5.2.]

Мы ограничимся наброском доказательства с помощью метода „отвинчивания"; можно было бы также действовать непосредственно, исходя из результатов приложения к гл. I или из результатов Вердье.

(i) *Случай* $A = \mathbf{Z}$.

Тогда $A' = \mathbf{G}_m$ и утверждение (а) следует из того, что $H^2(k, \mathbf{G}_m) = \mathbf{Q}/\mathbf{Z}$. Утверждение (б) получается из того, что $H^1(k, \mathbf{Z}) = 0$ и $H^1(k, \mathbf{G}_m) = 0$. Далее, так как $H^2(k, \mathbf{Z}) = \mathrm{Hom}(G_k, \mathbf{Q}/\mathbf{Z})$ и, согласно локальной теории полей классов (теорема „существования"), последняя группа двойственна пополнению группы k^* (в топологии, определенной открытыми подгруппами конечного индекса), то это доказывает (в).

(ii) *Случай* $A = \mathbf{Z}[G]$, *где* G — *конечная фактор-группа группы* G_k.

Так как G является группой Галуа некоторого конечного расширения K/k, то $H^i(k, A) = H^i(K, \mathbf{Z})$ и аналогично $H^i(k, A') = H^i(K, \mathbf{G}_m)$. Все сводится, следовательно, к предыдущему случаю (для поля K), разумеется, с проверкой коммутативности нужных диаграмм.

(iii) *Конечность* $H^1(k, A)$ *и* $H^1(k, A')$.

Конечность этих групп известна в случае, когда модуль A сам конечен (см. п. 5.2). Пользуясь „отвинчиванием“, можно свести, следовательно, задачу к случаю, когда модуль A свободен над $\mathbf{Z}$. Пусть K/k — расширение Галуа поля k с группой Галуа G, такое, что G_K действует тривиально на A. Тогда $H^1(K, A) = \mathrm{Hom}(G_K, A) = 0$ и аналогично $H^1(K, A') = 0$ (теорема 90). Поэтому

$$H^1(k, A) = H^1(G, A) \quad \text{и} \quad H^1(k, A') = H^1(G, A').$$

Очевидно, что группа $H^1(G, A)$ конечна; нетрудно доказывается также конечность группы $H^1(G, A')$ (см. гл. III, п. 4.3).

(iv) *Общий случай.*

Представим модуль A в виде фактора L/R, где L — свободный $\mathbf{Z}[G]$-модуль конечного типа, G — конечная факторгруппа группы G_k. Из рассуждений пункта (ii) следует, что теорема 6 справедлива для модуля L и, кроме того, $H^1(k, L) = H^1(k, L') = 0$. Каждая из точных последовательностей когомологий, соответствующих точным последовательностям модулей коэффициентов

$$0 \to R \to L \to A \to 0,$$
$$0 \to A' \to L' \to R' \to 0,$$

разбивается в таком случае на два куска. Таким образом получаются две коммутативные диаграммы (I) и (II), помещенные ниже. Для удобства записи мы опускаем букву k и обозначаем через E^* группу непрерывных гомоморфизмов топологической группы E в дискретную группу $\mathbf{Q}/\mathbf{Z}$; для топологических групп, которые мы будем рассматривать, „непрерывность“ оказывается эквивалентной „конечности порядка“. С учетом этого диаграммы, о которых идет речь, записываются в виде

$$\begin{array}{ccccccccc} 0 \to & H^1(R)^* & \to & H^0(A)^* & \to & H^0(L)^* & \to & H^0(R)^* & \to 0 \\ & f_1\uparrow & & f_2\uparrow & & f_3\uparrow & & f_4\uparrow & \\ 0 \to & H^1(R') & \to & H^2(A') & \to & H^2(L') & \to & H^2(R') & \to 0, \end{array} \qquad \text{(I)}$$

$$\begin{array}{ccccccccc} 0 \to & H^1(A) & \to & H^2(R) & \to & H^2(L) & \to & H^2(A) & \to 0 \\ & g_1\downarrow & & g_2\downarrow & & g_3\downarrow & & g_4\downarrow & \\ 0 \to & H^1(A')^* & \to & H^0(R')^* & \to & H^0(L')^* & \to & H^0(A')^* & \to 0. \end{array} \qquad \text{(II)}$$

Вертикальные стрелки определены здесь билинейными отображениями θ_i. Следует отметить к тому же, что строки этих диаграмм представляют собой *точные* последовательности. Это очевидно для диаграммы (I), а также для первой строки диаграммы (II). Что касается второй строки диаграммы (II), то нужно заметить, что функтор $\mathrm{Hom}_{\mathrm{cont}}(G, \mathbf{Q}/\mathbf{Z})$ точен на категории локально компактных абелевых групп, являющихся бесконечными (счетными) и вполне несвязными.

Теорема 6 теперь равносильна утверждению, что отображения f_2, g_1 и g_4 биективны. Но в силу сказанного в случае (ii) g_3 биективно. Отсюда следует сюръективность отображения g_4. Так как это рассуждение может быть применимо к любому G_k-модулю A, в частности к R, то получаем также сюръективность отображения g_2. Из этого и из диаграммы (II) следует, что g_4 биективно, так как биективно g_2. Наконец, g_1 также является биективным. В диаграмме (I) отображения f_1 и f_3 биективны. Отсюда вытекает, что f_2 инъективно, следовательно, инъективно также f_4, значит, f_2 биективно. Теорема доказана.

Замечание. В случае когда A — свободный $\mathbf{Z}$-модуль (иначе говоря, A' — тор), можно дать более простое доказательство теоремы 6, основанное на теоремах типа теоремы Тейта — Накаямы (см. [CL], гл. IX). Это доказательство приведено в заметках Ленга.

§ 6. ПОЛЯ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

На протяжении всего этого параграфа k будет обозначать некоторое *поле алгебраических чисел*, т. е. конечное расширение поля $\mathbf{Q}$. Точкой поля k называется класс эквивалентных нормирований поля k. Множество всех точек обозначим через V. Для любой точки $v \in V$ пополнение поля k относительно топологии, индуцированной точкой v, мы будем обозначать через k_v. Если v архимедова, то поле k_v изоморфно $\mathbf{R}$ или $\mathbf{C}$; если v неархимедова, то k_v — p-адическое поле.

6.1. Конечные модули, определение групп $P^i(k, A)$

Пусть A — коммутативная алгебраическая группа размерности 0 или, что то же самое, конечный G_k-модуль. Замена базы $k \to k_v$ позволяет определить группы когомологий $H^i(k_v, A)$, [если точка v архимедова, то условимся через $H^0(k_v, A)$ обозначать нульмерную группу когомологий Тейта (ср. [CL], гл. 8, п. 1) конечной группы G_{k_v} с коэффициентами в группе A[1]). Если, например, v — комплексная точка, то $H^0(k_v, A) = 0$].

Согласно п. 1.1, определены канонические гомоморфизмы

$$H^i(k, A) \to H^i(k_v, A).$$

Эти гомоморфизмы можно интерпретировать следующим образом. Пусть w — продолжение v до точки поля $\bar{k}$ и D_w — соответствующая группа разложения [$s \in D_w \Rightarrow$ $\Rightarrow s(w) = w$]. Обозначим через $\bar{k}_w$ объединение пополнений конечных подрасширений $\bar{k}$ (обращаем внимание, что оно *не совпадает* с пополнением поля $\bar{k}$ относительно топологии, индуцированной точкой w, ср. упражнение 1); легко доказывается, что $\bar{k}_w$ — алгебраическое замыкание поля k_v с группой Галуа D_w. Таким образом, группы $H^i(k_v, A)$ и $H^i(D_w, A)$ можно отождествить, и в этом случае гомоморфизм

$$H^i(k, A) \to H^i(k_v, A)$$

превращается просто в гомоморфизм ограничения

$$H^i(G_k, A) \to H^i(D_w, A).$$

Набор гомоморфизмов $H^i(k, A) \to H^i(k_v, A)$ определяет гомоморфизм $H^i(k, A) \to \prod H^i(k_v, A)$. На самом деле, прямое произведение можно заменить некоторой подгруппой. Более точно, пусть K/k — конечное расширение Галуа поля k, такое, что G_K тривиально действует на A, и пусть S — конечное множество точек поля k, содержащее все архимедовы точки, а также все точки, ветвящиеся в K.

---

[1]) См. также [M], гл. 12.— *Прим перев.*

Легко видеть, что если $v \notin S$, то G_{k_v}-модуль A неразветвлен в смысле п. 5.5 и определены подгруппы $H^i_{nr}(k_v, A)$. Пусть $P^i(k, A)$ — подгруппа произведения $\prod_{v \in V} H^i(k_v, A)$, состоящая из таких наборов (x_v), что x_v принадлежит группе $H^i_{nr}(k_v, A)$ почти для всех $v \in V$. Справедливо

Предложение 21. *Канонический гомоморфизм* $H^i(k, A) \to \prod H^i(k_v, A)$ *отображает группу* $H^i(k, A)$ в $P^i(k, A)$.

Действительно, каждый элемент $x \in H(k, A)$ определяется некоторым элементом $y \in H^i(L/k, A)$, где L/k — подходящее конечное расширение Галуа. Пусть T обозначает объединение множества S и множества точек поля k, ветвящихся в L. Легко видеть, что для всех $v \notin T$ образ x_v элемента x в группе $H^i(k_v, A)$ принадлежит подгруппе $H^i_{nr}(k_v, A)$. Это доказывает предложение.

Обозначим через f_i: $H^i(k, A) \to P^i(k, A)$ гомоморфизм, определенный в предыдущем предложении. Согласно предложению 18 из п. 5.5,

$$P^0(k, A) = \prod H^0(k_v, A),$$

$$P^2(k, A) = \coprod H^2(k_v, A) \text{ (прямая сумма).}$$

Что касается группы $P^1(k, A)$, то Тейт предложил обозначать ее через $\coprod\!\!\prod H^1(k_v, A)$, тем самым показывая, что она занимает промежуточное положение между прямым произведением и прямой суммой.

Наконец, группы $P^i(k, A)$, $i \geqslant 3$, являются просто произведениями (конечными) групп $H^i(k_v, A)$, где v пробегает множество *вещественных* архимедовых точек k. В частности, $P^i(k, A) = 0$ для $i \geqslant 3$, если поле k чисто мнимо или если A имеет нечетный порядок.

Замечание. Отображение f_0, очевидно, инъективно, и Тейт доказал (ср. п. 6.3), что гомоморфизмы f_i для $i \geqslant 3$ биективны. Напротив, f_1 и f_2 не обязательно инъективны (ср. гл. III, п. 4.7).

Упражнения. 1) Пусть w — некоторая точка алгебраического замыкания $\bar{k}$ поля k. Показать, что опреде-

ленное выше поле $\bar{k}_w$ неполно (заметить, что оно есть счетное объединение замкнутых подпространств без внутренних точек, и применить теорему Бэра). Показать, что пополнение поля $\bar{k}_w$ алгебраически замкнуто.

2) Определить группы $P^i(k, A)$ для отрицательных i. Показать, что система $\{P^i(k, A)\}_{i \in \mathbf{Z}}$ образует когомологический функтор от A.

6.2. Теорема собственности

Группы $P^i(k, A)$, определенные в предыдущем пункте, можно естественным образом снабдить топологией *локально компактной группы* (частный случай принадлежащего Браконьеру понятия „локальной прямой суммы“): возьмем за базис окрестностей нуля подгруппы $\prod_{v \notin T} H^i_{nr}(k_v, A)$, где T пробегает множество конечных частей V, содержащих S. Для группы $P^0(k, A) = \prod H^0(k_v, A)$ получаем топологию *произведения*, которая превращает $P^0(k, A)$ в *компактную* группу. Для группы $P^1(k, A) = \coprod H^1(k_v, A)$ получаем локально компактную топологию, а для $P^2(k, A) = \coprod H^2(k_v, A)$ — дискретную.

Теорема 7. *Если снабдить группу $H^i(k, A)$ дискретной топологией, а группу $P^i(k, A)$ — топологией, определенной выше, то канонический гомоморфизм*

$$f_i\colon H^i(k, A) \to P^i(k, A)$$

является собственным отображением[1]).

Мы докажем эту теорему только для $i = 1$. Случай $i = 0$ тривиален, а случай $i \geqslant 2$ следует из более точных теорем Тейта и Пуату, которые будут сформулированы в следующем пункте.

Пусть T — конечное подмножество множества V, содержащее S, и пусть $P^1_T(k, A)$ — подгруппа группы $P^1(k, A)$, образованная такими наборами (x_v), что $x_v \in H^1_{nr}(k, A)$

[1]) Непрерывное отображение топологических пространств называется *собственным*, если прообраз каждого компакта есть компакт. — *Прим. перев.*

для всех $v \notin T$. Ясно, что группа $P^1_T(k, A)$ компактна и что, наоборот, каждое компактное подмножество из $P^1(k, A)$ содержится в одной из групп $P^1_T(k, A)$. Достаточно, следовательно, доказать, что прообраз X_T группы $P^1_T(k, A)$ в $H^1(k, A)$ *конечен*. По определению элемент $x \in H^1(k, A)$ принадлежит X_T в том и только том случае, когда он „неразветвлен вне T". Обозначим, как и выше, через K/k конечное расширение Галуа поля k, такое, что G_K тривиально действует на A, и пусть T — множество точек из K, продолжающих точки из T. Легко видеть, что образ X_T в $H^1(K, A)$ состоит из элементов, неразветвленных вне T'; так как ядро отображения $H^1(k, A) \to H^1(K, A)$ конечно, все сводится, таким образом, к доказательству того, что этих элементов конечное число. Таким образом (если заменить k на K), можно считать, что G_k *действует тривиально на* A. В этом случае $H^1(k, A) = \mathrm{Hom}(G_k, A)$. Пусть $\varphi \in \mathrm{Hom}(G_k, A)$; обозначим через $k(\varphi)$ расширение поля k, соответствующее ядру φ; это расширение является абелевым, а φ определяет изоморфизм группы Галуа $G(k(\varphi)/k)$ на подгруппу группы A. Неразветвленность φ вне T означает, что расширение $k(\varphi)/k$ неразветвленно вне T. Так как степень расширений $k(\varphi)$ ограничена, теорема конечности, которую мы хотим доказать, вытекает из следующего более сильного результата:

Лемма 6. *Пусть k — поле алгебраических чисел, r — целое число и T — конечное множество точек поля k. Множество расширений степени r поля k, неразветвленных вне T, конечно.*

Доказательство немедленно сводится к случаю, когда $k = \mathbf{Q}$. Если E — расширение поля $\mathbf{Q}$ степени r, неразветвленное вне T, то дискриминант d поля E над $\mathbf{Q}$ делится только на простые числа, принадлежащие T. Кроме того, показатель степени p в d ограничен (это следует, например, из того, что у локального поля $\mathbf{Q}_p$ может быть только конечное число расширений степени, не превосходящей r, ср. гл. III, п. 4.2.). Таким образом, число возможных дискриминантов d конечно. Так как существует

только конечное число числовых полей с заданным дискриминантом (теорема Эрмита)[1]), это доказывает лемму.

6.3. Формулировки теорем Пуату и Тейта

В предыдущих обозначениях положим $A' = \mathrm{Hom}(A, \mathbf{G}_m)$. Теорема локальной двойственности вместе с предложением 19 п. 5.5 показывает, что *группа* $P^0(k, A)$ *двойственна группе* $P^2(k, A')$, а $P^1(k, A)$ *двойственна* $P^1(k, A')$ (следует только позаботиться об архимедовых точках, что удается благодаря соглашениям, принятым в начале п. 6.1). Следующие три теоремы значительно труднее. Мы ограничимся их формулировкой.

Теорема A. *Ядра отображений*

$$f_1\colon H^1(k, A) \to \prod H^1(k_v, A)$$

и

$$f_2'\colon H^2(k, A) \to \prod H^2(k_v, A')$$

двойственны друг другу.

Заметим, что этот результат, примененный к модулю A', устанавливает конечность ядра отображения f_2; отсюда немедленно следует случай $i = 2$ теоремы 7.

Теорема B. *Для* $i \geqslant 3$ *гомоморфизмы*

$$f_i\colon H^i(k, A) \to \prod H^i(k_v, A)$$

являются изоморфизмами.

Разумеется, можно ограничиться вещественными точками, т. е. такими, что $k_v = \mathbf{R}$.

Теорема C. *Имеет место точная последовательность*

$$0 \to \underset{\text{(конечна)}}{H^0(k, A)} \to \underset{\text{(компактна)}}{\prod H^0(k_v, A)} \to \underset{\text{(компактна)}}{H^2(k, A')^*} \to \underset{\text{(дискретна)}}{H^1(k, A)} \to \underset{\text{(лок. компактна)}}{\prod H^1(k_v, A)},$$

$$\to \underset{\text{(компактна)}}{H^1(k, A')^*} \to \underset{\text{(дискретна)}}{H^2(k, A)} \to \underset{\text{(дискретна)}}{\prod H^2(k_v, A)} \to \underset{\text{(конечна)}}{H^0(k, A')^*} \to 0$$

все гомоморфизмы в которой непрерывны.

---

[1]) См., например, Ленг [4*], гл. 5, § 4, теорема 5.— *Прим. перев.*

(Мы обозначаем через G^* группу, двойственную в смысле Понтрягина к локально компактной группе G.) Эти теоремы сформулированы в докладе Тейта в Стокгольме вместе с коротким наброском доказательства. Другие доказательства, принадлежащие Пуату, изложены в записках семинара в Лилле в 1963 г.

БИБЛИОГРАФИЧЕСКИЕ УКАЗАНИЯ К ГЛАВЕ II

Положение в точности аналогично ситуации в гл. I: почти все результаты принадлежат Тейту. Единственная публикация Тейта на эту тему — его доклад в Стокгольме, содержащий массу результатов (гораздо больше, чем мы могли здесь изложить), но очень мало доказательств. К счастью, доказательства в локальном случае были написаны Ленгом (размноженные записки); некоторые другие содержатся в докладе Дуади [1] на семинаре Бурбаки.

Следующие обстоятельства заслуживают упоминания:

1) На то, что понятие когомологической размерности (для группы Галуа G_k поля k) представляет интерес, впервые указал Гротендик в связи с его теорией „когомологий Вейля“[1]). Предложение 11 из п. 4.2 принадлежит ему.

2) Пуату получил результаты § 6 почти одновременно с Тейтом. Он опубликовал свои доказательства (которые, кажется, отличаются от доказательств Тейта) в семинаре в Лилле в 1963 г. (см. Пуату [1]).

3) Пуату и Тейт оба находились под влиянием результатов Касселса о когомологиях Галуа эллиптических кривых (см. доклад Касселса на конгрессе в Стокгольме).

---

[1]) О когомологиях Вейля — Гротендика алгебраических многообразий см. Манин [1*]. — *Прим. перев.*

ГЛАВА III

НЕКОММУТАТИВНЫЕ КОГОМОЛОГИИ ГАЛУА

Соглашение. Начиная с § 2, все рассматриваемые поля предполагаются совершенными.

§ 1. ФОРМЫ

Этот параграф посвящен иллюстрации одного общего „принципа", приблизительно формулируемого следующим образом.

Пусть K/k — расширение поля k, а X — некоторый „объект", определенный над k. Мы говорим, что объект Y, определенный над k, является *K/k-формой* объекта X, если Y становится изоморфен X при расширении основного поля до K. Классы таких форм (по отношению эквивалентности, определяемому k-изоморфизмами) образуют множество $E(K/k, X)$.

Если K/k — расширение Галуа, то можно установить биективное соответствие между множествами $E(K/k, X)$ и $H^1(G(K/k), A(K))$, где $A(K)$ обозначает группу K-автоморфизмов объекта X.

Очевидно, можно оправдать это утверждение, аксиоматически определив понятия „объекта, определенного над k", „расширения скаляров" и наложив на них некоторые простые требования. Я не отваживаюсь это делать и ограничусь обсуждением двух частных случаев: векторных пространств, снабженных тензорами, и алгебраических многообразий (или алгебраических групп). Читатель, интересующийся общим случаем, может обратиться к докладу 6 „Расслоенные категории и спуск" семинара Гротендика в 1961 г.

1.1. Тензоры

Этот пример подробно рассматривается в [CL], гл. 10, § 2. Напомним вкратце результат обсуждения.

„Объект" — это пара (V, x), где V — конечномерное векторное k-пространство, а x — фиксированный тензор на V типа (p, q), т. е. $x \in T_q^p(V) = T^p(V) \otimes T^q(V^*)$. Понятие k-изоморфизма двух объектов (V, x) и (V', x') ясно. Если K — расширение поля k и (V, x) — объект, определенный над k, то, взяв за V_K векторное пространство $V \otimes_k K$, а за x_K — элемент $x \otimes 1$ пространства $T_q^p(V_k) = T_q^p(V) \otimes_k K$, получим объект (V_K, x_K), определенный над K. Это однозначно определяет понятие K/k-формы, объекта (V, x); пусть $E(K/k)$ обозначает множество этих форм (с точностью до изоморфизма). Предположим, с другой стороны, что K/k — расширение Галуа, и пусть $A(K)$ — группа K-автоморфизмов объекта (V_K, x_K); если $s \in G(K/k)$ и $f \in A(K)$, то определим ${}^sf \in A(K)$ формулой

$$ {}^sf = (1 \otimes s) \circ f \circ (1 \otimes s^{-1}). $$

(Если f представляется матрицей (a_{ij}), то ${}^sf$ представляется матрицей $({}^sa_{ij})$.) Таким образом, на $A(K)$ вводится структура $G(K/k)$-группы и, значит, определено множество $H^1(G(K/k), A(K))$.

Пусть теперь (V', x') есть K/k-форма объекта (V, x). Множество k-изоморфизмов (V'_K, x'_K) на (V_K, x_K) естественным образом снабжается структурой главного однородного пространства над $A(K)$ и определяет тем самым элемент $p \in H^1(G(K/k), A(K))$, ср. гл. I, п. 5.2. Ставя в соответствие объекту (V', x') элемент p, получаем каноническое отображение

$$ \theta\colon E(K/k) \to H^1(G(K/k), A(K)). $$

Предложение 1. *Определенное выше отображение* θ *биективно.*

Доказательство дано в [CL][1]). Заметим только, что доказательство инъективности тривиально, а сюръективность вытекает из следующей леммы:

Лемма 1. *Для любого целого числа n имеет место равенство* $H^1(G(K/k), \mathbf{GL}_n(K)) = 0$.

(Для $n = 1$ получаем хорошо известную „теорему 90".)

Замечание. На самом деле группу $A(K)$ можно определить для любой коммутативной k-алгебры K; это группа K-точек некоторой алгебраической подгруппы A

---

[1]) Приведем доказательство этого утверждения. Прежде всего лемма 1 доказывается следующим образом.

Пусть $x \in K^n$, положим $b(x) = \sum_{s \in G} a_s x^s$, где $\{a_s\}$ есть 1-коцикл. Покажем, что векторы $b(x)$, $x \in K^n$, порождают все векторное пространство K^n. Действительно, если u — линейная форма, нулевая на всех $b(x)$, то для любого $h \in K$

$$0 = u(b(hx)) = \sum_{s \in G} a_s u(h^s x^s) = \sum_{s \in G} s(h)\, u(a_s x^s).$$

Так как для всех h мы получили линейную зависимость между $s(h)$, то в силу теоремы о линейной независимости автоморфизмов (Бурбаки [3*], гл. 5, § 7, п. 5) получаем, что $u(a_s x^s) = 0$, а поскольку a_s — обратимая матрица, отсюда следует, что $u = 0$.

Пусть теперь $x_1, \ldots, x_n$ — векторы из K^n, такие, что $y_i = b(x_i)$ линейно независимы. Обозначим через c матрицу перехода к базису, образованному x_i. Вычисляя соответствующую матрицу b, получаем $b(e_i) = y_i$, откуда следует, что b обратима. Остается воспользоваться тем же приемом, что и при доказательстве „теоремы 90" (см. примечание к стр. 91). Изложенное доказательство принадлежит П. Картье.

Покажем теперь *инъективность* отображения θ. Пусть (V'_1, x'_1) и (V'_2, x'_2) — две пары, соответствующие одному и тому же коциклу, и пусть f_1 и f_2 — соответствующие K-изоморфизмы. Тогда $f_1^{-1} s(f_1) = f_2^{-1} s(f_2)$, откуда $s(f_2 f_1^{-1}) = f_2 f_1^{-1}$, а это показывает, что отображение $f = f_2 f_1^{-1}$ является k-изоморфизмом (V'_1, x'_1) на (V'_2, x'_2).

Для доказательства *сюръективности* воспользуемся предыдущей леммой. Пусть p_s есть 1-коцикл группы G со значениями в $A(K)$; тогда $A(K) \subset \mathrm{GL}(V_K)$ и, применяя лемму,

группы $\mathbf{GL}(V)$. С матричной точки зрения уравнения, задающие группу A, получаются расписыванием соотношения $T_q^p(f)(x) = x$ [следует заметить, что так определяемая алгебраическая группа не обязательно „проста" над k (как схема) — ее структурный пучок может, например, иметь нильпотентные элементы (ср. п. 1.2, упражнение 2)] [1]). Как было принято в § 1 гл. II, мы будем писать $H^1(K/k, A)$ вместо $H^1(G(K/k), A(K))$.

Предыдущее предложение имеет дело только с *расширениями Галуа*. Следующее предложение часто позволяет сводить все к этому случаю:

Предложение 2. *Пусть* $\mathfrak{g}$ — *подалгебра Ли алгебры* $\mathfrak{gl}(V)$, *образованная элементами, оставляющими неподвижным тензор* x (*в инфинитезимальном смысле*, ср. Бурбаки [2], гл. I, § 3). *Для того чтобы алгебраическая группа автоморфизмов объекта* (V, x) *была гладкой над* k [2]), *необходимо и достаточно, чтобы ее размерность совпадала с размерностью* $\mathfrak{g}$. *При этом условии всякая* K/k-*форма* (V, x) *является также* k_s/k-*формой.*

получаем существование такого K-автоморфизма f пространства V_K, что

$$p_s = f^{-1}s(f) \quad \text{для всех} \quad s \in G.$$

Продолжим f до отображения тензорной алгебры V_K и положим $x' = f(x)$. Элемент x' принадлежит тензорной алгебре над k, так как

$$s(x') = s(f)(s(x)) = s(f)(x) = f \circ p_s(x) = f(x) = x'.$$

Отсюда следует, что (V, x') принадлежит $E(V/k)$ и ясно, кроме того, что образ этого элемента при отображении θ совпадает с классом коцикла p_s, что и требовалось доказать. — *Прим. перев.*

[1]) В случае если k — совершенное поле, „простота" схемы равносильна тому, что она неособая, т. е. что все ее локальные кольца регулярны. Для того чтобы избежать путаницы с термином „простая алгебраическая группа", Гротендик изменил термин „простая схема" на термин „гладкая схема". Этим термином мы и будем далее пользоваться. Заметим еще, что в случае $\operatorname{char} k = 0$ любая алгебраическая группа гладка (теорема П. Картье, см. Мамфорд [1*], лекция 25). В общем случае гладкость группы равносильна ее приведенности, т. е. отсутствию нильпотентных элементов в структурном пучке. — *Прим. перев.*

[2]) См. предыдущее замечание. — *Прим. перев.*

Пусть L — локальное кольцо группы A в ее единице, $\mathfrak{m}$ — его максимальный идеал. Легко заметить, что $\mathfrak{g}$ — не что иное, как касательное пространство к A в единице, т. е. двойственное пространство к $\mathfrak{m}/\mathfrak{m}^2$.

Так как $\dim(A) = \dim(L)$, получаем равенство $\dim(\mathfrak{g}) = \dim(A)$, которое означает, что L — регулярное кольцо или что группа A гладка над k в единице (а следовательно, и всюду, поскольку можно воспользоваться сдвигами). Это доказывает первое утверждение.

Пусть теперь (V', x') является K/k-формой объекта (V, x), а P — k-многообразие изоморфизмов (V', x') на (V, x). (Оставляем читателю заботу о его определении с помощью функтора или явных уравнений.) Из того что объекты (V', x') и (V, x) K-изоморфны, следует, что множество $P(K)$ непусто. Отсюда вытекает, что многообразия $P \otimes_k K$ и $A \otimes_k K$ K-изоморфны, в частности группа $P \otimes_k K$ гладка над K, откуда вытекает, что многообразие P гладко над k. В силу одного элементарного результата из алгебраической геометрии точки многообразия P со значением в k_s плотны в P[1]). Существования по крайней мере одной такой точки достаточно, чтобы убедиться, что объекты (V, x) и (V', x') k_s-изоморфны, что и требовалось доказать.

1.2. Примеры

(а) Возьмем за тензор x знакопеременную невырожденную билинейную форму. Группа A есть симплектическая группа $\mathbf{Sp}$, отнесенная к этой форме. С другой стороны, элементарная теория знакопеременных форм показывает, что все формы x тривиальны (т. е. изоморфны x). Отсюда получаем

Предложение 3. *Для любого расширения Галуа K/k имеет место равенство* $H^1(K/k, \mathbf{Sp}) = 0$.

(б) Предположим, что характеристика отлична от 2 и возьмем за x невырожденную симметрическую билинейную форму. Группа A — *ортогональная* группа $\mathbf{O}(x)$, соответствующая x. Отсюда получаем

---

[1]) См., например, Дьедонне [2*], стр. 82. — *Прим. перев.*

Предложение 4. *Для любого расширения Галуа K/k множество $H^1(K/k, \mathbf{O}(x))$ находится в биективном соответствии с множеством квадратичных форм над k, которые K-эквивалентны x.*

При $p=2$ надо заменить билинейную симметрическую форму на квадратичную форму, что вынуждает покинуть рамки тензорных пространств (ср. упражнение 2).

(в) Возьмем за x тензор типа (1,2), или, что сводится к тому же, структуру *алгебры* на пространстве V. Группа A в таком случае есть группа автоморфизмов этой алгебры, а алгебра $\mathfrak{g}$ — алгебра Ли ее *дифференцирований*. В случае когда $V=\mathbf{M}_n(k)$, K/k-формы V — это просто центральные простые алгебры ранга n^2 над k, распадающиеся над K; группа A отождествляется с проективной группой $\mathbf{PGL}_n(k)$. Это дает интерпретацию множества $H^1(K/k, \mathbf{PGL}_n)$ в терминах простых алгебр, ср. [CL], гл. 10, § 5.

Упражнения. 1) Показать, что всякое дифференцирование алгебры $\mathbf{M}_n(k)$ внешнее. Воспользовавшись этим фактом, а также предложением 2, доказать теорему, согласно которой каждая центральная простая алгебра обладает полем разложения, являющимся расширением Галуа основного поля.

2) Пусть V — векторное пространство над полем характеристики 2, F — квадратичная форма на V, а $\langle a, b\rangle$ — соответствующая билинейная форма. Показать, что алгебра Ли $\mathfrak{g}$ ортогональной группы $\mathbf{O}(F)$ образована такими эндоморфизмами u пространства V, что $\langle a, u(a)\rangle=0$ для любого a. Вычислить размерность алгебры $\mathfrak{g}$, предполагая, что форма $\langle a, b\rangle$ невырождена (что дает $\dim V\equiv 0 \bmod 2$), получить отсюда для этого случая простоту группы $\mathbf{O}(F)$. Останется ли этот результат верным для вырожденной формы $\langle a, b\rangle$?

1.3. Алгебраические многообразия, группы и т. д.

Возьмем теперь в качестве объекта *алгебраическое многообразие* (соответственно алгебраическую группу или алгебраическое однородное пространство над алгебраической группой). Пусть V — такое многообразие, определенное над полем k, и K/k — расширение k; обозначим

через $A(K)$ группу K-автоморфизмов многообразия $V \underset{k}{\otimes} K$ (снабженного в случае необходимости своей структурой группы, соответственно однородного пространства). Таким образом, получаем функтор Aut_V, удовлетворяющий аксиомам гл. II, § 1.

Пусть теперь K/k — расширение Галуа поля k и V' является K/k-формой многообразия V. Множество P K-изоморфизмов $V' \underset{k}{\otimes} K$ на $V \underset{k}{\otimes} K$ является, очевидно, главным однородным пространством относительно $G(K/k)$-группы $A(K) = \mathrm{Aut}_V(K)$. Таким образом, как и в п. 1.1, определено каноническое отображение

$$\theta\colon E(K/k, V) \to H^1(K/k, \mathrm{Aut}_V).$$

Предложение 5. *Отображение* θ *инъективно; если, кроме того, многообразие* V *квазипроективно, то оно биективно.*

Инъективность θ тривиальна. Для доказательства сюръективности (в случае когда V квазипроективно) применяем метод „спуска основного поля“ Вейля, который сводится просто к следующему [1]).

Предположим для простоты, что K/k конечно, и пусть $c = (c_s)$ есть 1-коцикл группы $G(K/k)$ со значениями в $\mathrm{Aut}_V(K)$. Беря композицию c_s с автоморфизмами $1 \otimes s$ многообразия $V \underset{k}{\otimes} K$, заставим действовать группу $G(K/k)$ на $V \underset{k}{\otimes} K$; тогда фактормногообразие

$${}_cV = (V \underset{k}{\otimes} K)/G(K/k)$$

определяет K/k-форму V. (Этот фактор существует, так как V предполагается квазипроективным [2]).) Говорят, что ${}_cV$ получается *скручиванием многообразия* V *с помощью коцикла* c (эта терминология явно соответствует терминологии гл. I, п. 5.3). Легко видеть, что образ ${}_cV$ при отображении θ равен классу когомологий коцикла c; отсюда следует сюръективность отображения θ.

---

[1]) См. Серр [6*], гл. 5. — *Прим. перев.*

[2]) См. Серр [6*], гл. 3, п. 11. — *Прим. перев.*

Следствие. *Если V — алгебраическая группа, то отображение θ биективно.*

Действительно, известно, что всякое многообразие группы квазипроективно [1]).

Замечания. 1. Предложение 5 показывает, что K/k-формы двух многообразий V и W, определяющих *одинаковый функтор автоморфизмов*, находятся в биективном соответствии (K — расширение Галуа поля k). Примеры:

Алгебры октав	$\Leftrightarrow$	Простые группы типа $\mathbf{G}_2$.
Простые центральные алгебры ранга n^2	$\Leftrightarrow$	Многообразия Севери — Брауэра размерности $n-1$.
Полупростые алгебры с инволюцией	$\Leftrightarrow$	Классические группы с тривиальным центром.

2. Функтор Aut_V *не всегда представим* (в категории k-схем); более того, даже если он представим, может случиться, что представляющая его схема не имеет конечного типа над k, т. е. не определяет „алгебраической группы" в обычном смысле этого термина.

§ 2. ПОЛЯ, РАЗМЕРНОСТЬ КОТОРЫХ НЕ ПРЕВОСХОДИТ 1

Напомним, что теперь поле k предполагается *совершенным*. Под „алгебраическими группами" мы будем понимать *приведенные* групповые схемы *конечного типа* над полем k (это в точности „алгебраические группы" Вейля, только не обязательно связные).

Если A — алгебраическая группа, то вместо $H^1(\bar{k}/k, A)$ мы будем писать $H^1(k, A)$ (где $\bar{k}$ означает алгебраическое замыкание k).

2.1. Общие сведения о линейных группах

(Библиография: Борель [1], Розенлихт [1] и [2], Шевалле [3].)

Алгебраическая группа L называется линейной, если она изоморфна подгруппе группы $\mathbf{GL}_n$, это эквивалентно

---

1) См., например, Чоу [1*]. — *Прим. перев.*

тому, что соответствующее алгебраическое многообразие *аффинно.*

Линейная группа U называется *унипотентной*, если при погружении в $\mathbf{GL}_n$ все ее элементы унипотентны (это не зависит от выбора погружения). Для этого необходимо и достаточно, чтобы все последовательные факторы ее композиционного ряда были изоморфны аддитивной группе $\mathbf{G}_a$ или группе $\mathbf{Z}/p\mathbf{Z}$ (p — характеристика k). Эти группы мало интересны с когомологической точки зрения.

Предложение 6. *Если U — связная линейная унипотентная группа, то $H^1(k, U) = 0$.*

(Этот результат не переносится на случай несовершенного основного поля, ср. упражнение.)

Это следует из того, что $H^1(k, \mathbf{G}_a) = 0$ (гл. II, предложение 1). Линейная группа T называется *тором*, если она изоморфна над $\bar{k}$ произведению мультипликативных групп. Эти группы определяются, с точностью до изоморфизма, своей *группой характеров* $X(T) = \mathrm{Hom}(T, \mathbf{G}_m)$, являющейся свободным $\mathbf{Z}$-модулем конечного ранга, на котором непрерывно действует $G(\bar{k}/k)$.

Каждая связная разрешимая линейная группа R содержит максимальную унипотентную подгруппу U, являющуюся нормальным делителем в G. Факторгруппа $T = R/U$ есть тор, и R является полупрямым произведением U на T. (Это разложение справедливо над основным полем.)

Всякая линейная группа L содержит максимальный связный разрешимый нормальный делитель R, который называется *радикалом* группы. В случае если $R = 0$ и L связна, говорят, что L *полупроста*; в общем случае связная компонента единицы $(L/R)_0$ группы L/R полупроста.

Таким образом, каждая линейная группа обладает композиционным рядом, последовательные факторы которого принадлежат к одному из следующих четырех типов: $\mathbf{G}_a$, тор, конечная группа и полупростая группа.

Подгруппа P группы L называется *параболической*, если L/P — *полное* многообразие; если, кроме того, P разрешима и связна, то говорят, что P — *борелевская* подгруппа в L. Всякая параболическая подгруппа содержит радикал R группы L.

10 Зак. 1202

Предположим, что поле k алгебраически замкнуто, а группа L связна. Борелевские подгруппы B группы L характеризуются одним из следующих свойств:

а) максимальная связная разрешимая подгруппа группы L,

б) минимальная параболическая подгруппа группы L. Кроме того, борелевские подгруппы сопряжены между собой и совпадают со своими собственными нормализаторами. (Отметим, что если поле k не является алгебраически замкнутым, в группе L может не существовать никакой борелевской подгруппы, определенной над k, ср. п. 2.2.)

Подгруппа C линейной группы называется *картановской подгруппой*, если она нильпотентна и совпадает со связной компонентой единицы своего нормализатора. Существует по крайней мере одна картановская подгруппа, определенная над полем k, и все эти подгруппы сопряжены (над полем $\bar{k}$, но в общем случае не над k). В случае когда группа L полупроста, картановские подгруппы совпадают с *максимальными торами.*

Упражнение. Пусть k_0 — поле характеристики p и $k = k_0((t))$ — поле формальных степенных рядов от одной переменной над k_0. Это поле несовершенно; в случае если k_0 алгебраически замкнуто, размерность этого поля не превосходит 1 (а также оно обладает свойством (C_1), ср. гл. II, п. 3.2).

Пусть U — подгруппа из $\mathbf{G}_a \times \mathbf{G}_a$, образованная парами (y, z), удовлетворяющими уравнению $y^p - y = tz^p$. Показать, что это связная унипотентная группа размерности 1, гладкая над k. Вычислить $H^1(k, U)$ и показать, что эта группа отлична от нуля, если $p \neq 2$. Взяв уравнение $y^2 + y = tz^4$, показать, что в характеристике 2 имеет место аналогичный результат.

2.2. Тривиальность H^1 для связных линейных групп

Теорема 1. *Пусть k — поле. Следующие 4 условия эквивалентны:*

(i) $H^1(k, L) = 0$ *для любой связной алгебраической линейной группы L;*

(i′) $H^1(k, L) = 0$ *для любой полупростой алгебраической группы L;*

(ii) *всякая линейная алгебраическая группа содержит борелевскую подгруппу, определенную над* k;

(ii′) *каждая полупростая алгебраическая группа* L *содержит борелевскую подгруппу, определенную над* k.

Кроме того, из этих свойств следует, что $\dim(k) \leqslant 1$ (ср. гл. II, § 3).

(Напомним, что все рассматриваемые поля предполагаются совершенными.)

Доказываем в несколько шагов:

(1) (ii)$\Rightarrow$(ii′). Это тривиально.

(2) (ii′)$\Rightarrow \dim(k) \leqslant 1$. Действительно, пусть D — тело, центр которого является конечным расширением k' поля k. Элементы из D, приведенная норма которых равна 1, являются рациональными точками над k полупростой алгебраической группы $\mathbf{SL}(D)$. Если $D \neq k'$, то эта группа не совпадает с $\{1\}$ и условие (ii′) показывает, что она содержит борелевскую подгруппу, определенную над k, а следовательно, по крайней мере один унипотентный элемент, отличный от 1, что, очевидно, невозможно.

Таким образом, $D = k'$, откуда явно следует, что $\dim(k) \leqslant 1$.

(3) (i′)$\Rightarrow \dim(k) \leqslant 1$. Пусть K — конечное расширение поля k. Для всякой алгебраической группы L, определенной над K, можно построить (ср. Вейль [4], стр. 4) алгебраическую группу $R_{K/k}(L)$ над k (точки этой группы со значением в $\bar{k}$ образуют „индуцированный модуль“ для группы $L(\bar{k})$, определение которого было дано в гл. I, п. 5.8). Имеет место равенство

$$H^1(K, L) = H^1(k, R_{K/k}(L)).$$

Если группа L полупроста, то и группа $R_{K/k}(L)$ полупроста, а следовательно, в силу свойства (i′) $H^1(K, L) = 0$. Применяя это к группе $\mathbf{PGL}_n$ (n произвольно), получаем, что группа Брауэра поля K равна 0, откуда $\dim(k) \leqslant 1$.

(4) $\dim(k) \leqslant 1 \Rightarrow H^1(k, R) = 0$, *если группа* R *разрешима*. Группа R является расширением тора с помощью унипотентной группы. Так как группа когомологий последней равна 0, мы видим, что все сводится к случаю,

когда R — *тор*, этот случай рассматривается в [CL], стр. 170 [1]).

(5) (i) $\Leftrightarrow$ (i′). Импликация (i) $\Rightarrow$ (i′) тривиальна. Предположим, что выполнено (i′). В силу результатов пунктов (3) и (4) для разрешимой группы R имеет место равенство $H^1(k, R) = 0$, и, воспользовавшись точной последовательностью групп H^1, получаем утверждение (i).

(6) (i′) $\Leftrightarrow$ (ii′). Воспользуемся следующей леммой:

Лемма 1. *Пусть A — алгебраическая группа, H — ее подгруппа, N — нормализатор H в A. Пусть c — некоторый 1-коцикл группы $G(\bar{k}/k)$ со значениями в $A(\bar{k})$, а $x \in H^1(k, A)$ — соответствующий класс когомологий. Обозначим через ${}_cA$ алгебраическую группу, полученную скручиванием A с помощью c (A действует на себе внутренними автоморфизмами.) Следующие два условия эквивалентны:*

(а) *элемент x принадлежит образу отображения $H^1(k, N) \to H^1(k, A)$;*

(б) *группа ${}_cA$ содержит подгруппу H', определенную над k и сопряженную подгруппе H (над алгебраическим замыканием $\bar{k}$ поля k).*

Это простое следствие предложения 37 гл. I, примененного к вложению N в A; надо просто заметить, что точки факторгруппы A/N находятся в биективном соответ-

---

[1]) Пусть R — тор над k. Обозначим его группу характеров через X. Пусть K/k — расширение Галуа, достаточно большое, чтобы все элементы $x \in X$ были рациональны над K (см. примечание на стр. 152). Группа $R(K)$ точек R над K канонически отождествляется с $K^* \otimes X'$, где $X' = \mathrm{Hom}(X, \mathbf{Z})$. Когомологическая тривиальность модуля K^* эквивалентна тому, что проективная размерность $\mathbf{Z}(G)$-модуля K^* не больше единицы. Таким образом, существует проективная резольвента

$$0 \to P_1 \to P_0 \to K^* \to 0.$$

Тензорно умножая ее на X', получаем, поскольку X' — свободный Z-модуль, что

$$0 \to P_1 \otimes X' \to P_0 \otimes X' \to K^* \otimes X' \to 0.$$

Так как модули $P_i \otimes X'$ ($i = 0, 1$) слабо проективны (см. [M], гл. 10, предложение 8.1), модули $K^* \otimes X'$ когомологически тривиальны; таким образом, $H^1(K, R(K)) = 0$. — *Прим. перев.*

ствии с подгруппами из A, сопряженными H, и то же самое относится к $_c(A/N)$.

Вернемся к доказательству (i′) $\Leftrightarrow$ (ii′). Если выполнено условие (ii′), то, применяя лемму 1 к борелевской подгруппе B полупростой группы L, мы видим, что отображение $H^1(k, B) \to H^1(k, L)$ сюръективно. Так как в силу пунктов (2) и (4) $H^1(k, B) = 0$, сразу же получаем, что $H^1(k, L) = 0$. Наоборот, предположим, что выполнено свойство (i′), и пусть L — полупростая группа. Сразу же все сводится к случаю, когда *центр* L тривиален (центр определяется как групповая подсхема, не обязательно приведенная), другими словами, когда L — *присоединенная группа*. Как доказал Шевалле (ср. также Демазур, Гротендик [1]), существует *форма* L_d группы L, которая *расщепима*[1]), и L получается из L_d скручиванием с помощью класса $x \in H^1(k, \mathrm{Aut}(L_d))$. Структура группы $\mathrm{Aut}(L_d)$ определена Шевалле; она является полупрямым произведением группы L_d на конечную группу E, изоморфную группе автоморфизмов соответствующей схемы Дынкина.

Принимая во внимание условие (i′), мы видим, что группу $H^1(k, \mathrm{Aut}(L_d))$ можно отождествить с $H^1(k, E)$. Но элементы группы E (отождествленные с подгруппами из $\mathrm{Aut}(L_d)$), сохраняют борелевскую подгруппу B группы L_d; таким образом, обозначая через N нормализатор B в $\mathrm{Aut}(L_d)$, мы приходим к выводу, что отображение

$$H^1(k, N) \to H^1(k, \mathrm{Aut}(L_d))$$

сюръективно. Применяя лемму 1, получаем, что L содержит борелевскую подгруппу, определенную над k, что и требовалось доказать.

Замечание. Полупростые группы, содержащие борелевскую подгруппу, определенную над k, называются *квазирасщепимыми*; см. по этому поводу Титц [1].

---

[1]) Алгебраическая разрешимая группа H над k называется k-расщепимой, если она связна и обладает композиционным рядом $H = H_0 \supset H_1 \supset \ldots \supset H_t = \{1\}$, где H_i — связные подгруппы, определенные над k, а факторы H_i/H_{i+1} k-изоморфны группам k^+ или k^*. Произвольная алгебраическая группа называется расщепимой, если она содержит расщепимую борелевскую подгруппу. — *Прим. перев.*

Теорема 2. *Если k — поле характеристики нуль, то четыре условия теоремы* 1 *эквивалентны двум следующим:*

(iii) *всякая полупростая алгебраическая группа, не совпадающая с* $\{1\}$, *содержит унипотентный элемент, отличный от* 1;

(iii′) *каждая полупростая алгебра Ли* $\mathfrak{g} \neq 0$ *содержит отличный от нуля нильпотентный элемент.*

Эквивалентность условий (iii) и (iii′) следует из теории Ли. Импликация (ii′) $\Rightarrow$ (iii) тривиальна. Для доказательства обратной импликации рассуждаем индукцией по размерности полупростой группы L. Можно считать, что $L \neq 0$. Выберем минимальную параболическую подгруппу P группы L, определенную над k (ср. Годеман [1]), и пусть R — ее радикал. Факторгруппа P/R полупроста и не содержит унипотентных элементов, отличных от 1. Ее размерность строго меньше размерности L, так как L содержит по крайней мере один унипотентный элемент, отличный от 1 (Годеман [1], теорема 9). По предположению индукции $P = R$, а это означает, что P — борелевская подгруппа группы L.

Замечание. Как показал недавно Титц, условие (iii) эквивалентно условиям (i), (i′), (ii), (ii′), даже если характеристика k отлична от нуля (поле k, как всегда, предполагается совершенным).

2.3. Гипотеза

Она состоит в том, что справедливо утверждение, обратное к теореме 1. Другими словами,

Гипотеза 1. *Если* $\dim(k) \leqslant 1$, *то выполняются эквивалентные свойства* (i), (i′), (ii), (ii′), *сформулированные в теореме* 1.

Эта гипотеза мне кажется чрезвычайно правдоподобной. В следующих двух случаях она уже доказана:

а) *Когда k — конечное поле* (Ленг).

Справедлив даже более сильный результат: $H^1(k, G) = 0$ для любой связной алгебраической группы (не обязательно линейной). Доказательство состоит в простом применении свойств эндоморфизма Фробениуса, см. Ленг [2].

б) *Когда* k — *поле типа* (C_1) *характеристики нуль* (Спрингер).

Воспользовавшись теоремой 2, мы видим, что достаточно доказать, что не существует ненулевой полупростой алгебры Ли $\mathfrak{g}$, все элементы которой полупросты. Пусть это не так, очевидно, можно считать, что размерность n алгебры $\mathfrak{g}$ минимальна. Пусть r — ранг $\mathfrak{g}$. Если $x \in \mathfrak{g}$, то характеристический многочлен $\det(T - \mathrm{ad}(x))$ делится на T^2; пусть $f_r(x)$ — его коэффициент при T^r. Очевидно, что f_r — полиномиальная функция степени $n - r$ на алгебре $\mathfrak{g}$. Так как k — поле типа (C_1), отсюда следует, что в $\mathfrak{g}$ существует такой элемент x, что $f_r(x) = 0$. Пусть $\mathfrak{c}$ — централизатор x в $\mathfrak{g}$; поскольку элемент x полупрост, тот факт, что $f_r(x)$ отличен от нуля, означает, что $\dim(\mathfrak{c}) > r$. Так как $x \neq 0$, то $\dim(\mathfrak{c}) < n$. Известно (ср. Бурбаки [2] гл. I, § 6, п. 5), что $\mathfrak{c}$ есть произведение коммутативной алгебры на полупростую. По предположению индукции последняя алгебра должна быть нулевой, следовательно, $\mathfrak{c}$ коммутативна, откуда получаем неравенство $\dim(\mathfrak{c}) \leqslant r$ и тем самым противоречие.

В общем случае при наличии только условия $\dim(k) \leqslant 1$ удается лишь доказать, что $H^1(k, L) = 0$ для классической полупростой группы L (не содержащей множителей типа $\mathbf{D}_4$). Доказательство легкое (ср. Серр [2], стр. 59—63), и его не имеет смысла здесь приводить. Случай особых групп $\mathbf{G}_2$, $\mathbf{F}_4$ и $\mathbf{E}_6$ по крайней мере, когда характеристика отлична от 2 и 3, разбирается аналогичным образом (ср. Спрингер [3]).

Титц указал мне способ, позволяющий в принципе разобраться со случаем $\mathbf{E}_7$, однако остается группа $\mathbf{E}_8$. Впрочем, я надеюсь, что эти проверки отдельных случаев окажутся ненужными и что будет найдено *априорное* доказательство гипотезы 1 [1]).

---

[1]) Эта гипотеза доказана Штейнбергом как следствие такой теоремы: пусть L — полупростая односвязная группа, определенная над совершенным полем k. Предположим, что L содержит борелевскую подгруппу, определенную над k. Для любого элемента $x \in H^1(k, L)$ существует максимальный тор T группы L, определенный над k и такой, что x лежит в образе $H^1(k, T)$ в группе $H^1(k, L)$. (Если $\dim(k) \leqslant 1$, то $H^1(k, T) = 0$, откуда $H^1(k, L) = 0$. Переход к случаю произвольной связной линейной группы не представляет труда.) См. Штейнберг [1].

Упражнение. Пусть $\mathfrak{g}$ — простая алгебра Ли над полем k характеристики 0. Пусть n (соответственно r) — размерность (соответственно ранг) алгебры $\mathfrak{g}$. Известно (ср. Констант [1]), что множество $\mathfrak{g}_u$ нильпотентных элементов из $\mathfrak{g}$ совпадает с множеством общих нулей r однородных многочленов $F_1, \ldots, F_r$ степеней $m_1, \ldots, m_r$ соответственно, для которых

$$m_1 + m_2 + \ldots + m_r = \frac{n+r}{2}.$$

Воспользоваться этим фактом для доказательства того, что $\mathfrak{g}_u \neq 0$ для поля k, удовлетворяющего условию (C_1).

2.4. Рациональные точки однородных пространств

Результаты и гипотезы предыдущих пунктов относились к первому множеству когомологий H^1, т. е. к главным однородным пространствам. Следующая теорема, принадлежащая Спрингеру, позволяет перейти к произвольным однородным пространствам.

Теорема 3. *Пусть k — поле, размерность которого не превосходит 1, A — алгебраическая группа и X — однородное пространство (правое) над A. Тогда существует главное однородное пространство P над A и A-гомоморфизм π: $P \to X$.*

(Само собой разумеется, что A, X, P, π предполагаются определенными над k.)

Прежде чем доказывать эту теорему, сформулируем несколько следствий:

Следствие 1. *Предположим, что $\dim(k) \leqslant 1$ и что $H^1(k, A) = 0$. Тогда каждое однородное пространство X над A имеет рациональную точку*[1]. *Действительно, главное однородное пространство P должно быть тривиально, следовательно, оно имеет рациональную точку p; образ этой точки при отображении π определяет рациональную точку X.*

---

[1]) Пусть X — многообразие, определенное над полем k. Точка $x \in X$ называется рациональной, если все ее координаты принадлежат полю k. — *Прим. перев.*

Этот результат, в частности, применим, когда *поле* k *удовлетворяет условиям* (i), (i′), (ii), (ii′) *теоремы* 1 *и* A — *связная линейная группа.*

Следствие 2. *Предположим, что* $\dim(k) \leqslant 1$, *и пусть* $f\colon A \to A'$ — *сюръективный гомоморфизм алгебраических групп. Соответствующее отображение* $H^1(k, A) \to H^1(k, A')$ *сюръективно.*

Пусть $x' \in H^1(k, A')$, а P' — главное однородное пространство над A', соответствующее x'. Заставим действовать A на P' с помощью f, снабдив тем самым P' структурой однородного пространства над A. В силу теоремы 3 существует главное однородное пространство P над A и A-гомоморфизм $\pi\colon P \to P'$. Пусть $x \in H^1(k, A)$ — класс пространства P. Легко проверяется, что образ x в $H^1(k, A')$ равен x', что и требовалось доказать.

Следствие 3. *Пусть* k — *поле, удовлетворяющее условиям* (i), (i′), (ii), (ii′) *теоремы* 1, и L — *линейная алгебраическая группа, определенная над* k. *Обозначим через* L_0 *связную компоненту единицы группы* L. *Каноническое отображение*

$$H^1(k, L) \to H^1(k, L/L_0)$$

биективно.

Следствие 2 показывает, что это отображение сюръективно. С другой стороны, пусть c есть 1-коцикл группы $G(\bar{k}/k)$ со значениями в $L(\bar{k})$ и ${}_cL_0$ — группа, полученная скручиванием подгруппы L_0 с помощью c (это имеет смысл, так как L действует на L_0 внутренними автоморфизмами); поскольку группа ${}_cL_0$ — связная линейная группа, условие (i) показывает, что $H^1(k, {}_cL_0) = 0$. Воспользовавшись точной последовательностью неабелевых когомологий (ср. гл. I, п. 5.5, следствие 2 к предложению 3.9), получаем, что отображение $H^1(k, L) \to H^1(k, L/L_0)$ инъективно, что и требовалось доказать. Тем самым когомологии линейных групп полностью сводятся к когомологиям *конечных* групп.

Доказательство теоремы 3. Возьмем точку $x \in X(\bar{k})$. Для любого $s \in G(\bar{k}/k)$, ${}^s x \in X(\bar{k})$, а значит, существует $a_s \in A(\bar{k})$, такой, что ${}^s x = x \cdot a_s$. Легко видеть, что (a_s)

непрерывно зависит от s, другими словами, определяет 1-*коцепь группы* $G(\bar{k}/k)$ *со значениями* в $A(\bar{k})$. Если бы коцепь (a_s) была коциклом, то можно было бы найти главное однородное пространство P над A и точку $p \in P(\bar{k})$, такую, что ${}^s p = p \cdot a_s$; положив $\pi(p \cdot a) = xa$, мы получили бы A-гомоморфизм π: $P \to X$, отвечающий нужным условиям. Таким образом, все сводится к доказательству следующего предложения:

Предложение 7. *В предыдущих условиях можно так выбрать* 1-*коцепь* (a_s), *чтобы она была коциклом.*

Рассмотрим системы $\{H, (a_s)\}$, образованные алгебраической подгруппой H группы A (определенной над $\bar{k}$) и 1-коциклом (a_s) группы $G(\bar{k}/k)$ со значениями в $A(\bar{k})$, для которых выполняются следующие условия:

1) $x \cdot H = x$ (*H содержится в стабилизаторе x*);

2) ${}^s x = x \cdot a_s$ *для всех* $s \in G(\bar{k}/k)$;

3) *для любых двух элементов* $s, t \in G(\bar{k}/k)$ *существует такой* $h_{s,t} \in H(\bar{k})$, *что* $a_s \cdot {}^s a_t = h_{s,t} \cdot a_{st}$;

4) $a_s \cdot {}^s H \cdot a_s^{-1} = H$ *для всех* $s \in G(\bar{k}/k)$.

Лемма 2. *Существует по крайней мере одна система* $\{H, (a_s)\}$.

Возьмем за H стабилизатор элемента x, а за (a_s) — любую коцепь, удовлетворяющую условию 2. Так как $x \cdot a_s \cdot {}^s a_t = {}^{st} x = x a_{st}$, существует $h_{s,t} \in H(\bar{k})$, такой, что $a_s \cdot {}^s a_t = h_{s,t} \cdot a_{st}$, откуда получаем условие 3. Свойство 4 выводится немедленно.

Выберем теперь систему $\{H, (a_s)\}$, в которой H *минимальна*. Остается теперь установить, что H совпадает с $\{1\}$, действительно, условие 3 покажет тогда, что (a_s) — коцикл.

Лемма 3. *Если подгруппа H минимальна, то связная компонента единицы H_0 группы H разрешима.*

Пусть L — максимальная связная линейная подгруппа в H_0. Согласно одной теореме Шевалле, L — нормальный делитель H_0, а факторгруппа H_0/L является абелевым многообразием[1]). Пусть B — борелевская подгруппа в L

---

[1]) См. Розенлихт [1]. — *Прим. перев.*

и N — ее нормализатор в H. Покажем, что $N = H$, откуда будет следовать, что B — нормальный делитель L, а следовательно, совпадает с L. Это, очевидно, показывает, что H_0 разрешима (как расширение абелева многообразия с помощью B).

Пусть $s \in G(\bar{k}/k)$. Очевидно, ${}^sB$ — борелевская подгруппа ${}^sL$, которая является максимальной связной линейной подгруппой в ${}^sH_0$. Отсюда следует, что $a_s {}^sB \cdot a_s^{-1}$ — борелевская подгруппа группы $a_s {}^sLa_s^{-1}$, которая совпадает с L (так как она максимальная связная линейная подгруппа группы $a_s {}^sH_0 \cdot a_s^{-1} = H_0$). Сопряженность борелевских подгрупп показывает, следовательно, что существует такой элемент $h_s \in L$, что $h_s \cdot a_s {}^sB \cdot a_s{}^{-1} h_s^{-1} \in B$; очевидно, можно считать, что h_s непрерывно зависит от s. Положим $a'_s = h_s \cdot a_s$. В этом случае *система* $\{N, (a'_s)\}$ *удовлетворяет условиям* 1, 2, 3 и 4. Действительно, свойства 1 и 2 очевидны. Для доказательства 3 определим $h'_{s,t}$ формулой

$$a'_s \cdot {}^sa'_t = h'_{s,t} \cdot a'_{st}.$$

Легкие вычисления показывают, что

$$h_s \cdot a_s {}^sh_t \cdot a_s^{-1} h_{s,t} = h'_{t,t} \cdot h_{s,t}.$$

Поскольку $a_s {}^sh_t a_s^{-1} \in a_s {}^sH \cdot a_s^{-1} = H$, из этой формулы следует, что $h'_{s,t}$ принадлежит H. С другой стороны, по построению, $a'_s {}^sBa'^{-1}_s = B$. Отсюда следует, что каждый из внутренних автоморфизмов, определяемых элементами a^s_{st} и $a'_s {}^sa'_t$, преобразует ${}^{st}B$ в B; внутренний автоморфизм, определяемый частным $h'_{s,t}$, преобразует, следовательно, группу B в себя, а это, очевидно, показывает, что $h'_{s,t}$ принадлежит N, и доказывает (3). Наконец, поскольку внутренний автоморфизм, определяемый a'_s, преобразует ${}^sB$ в B, он преобразует также ${}^sN$ в N, что доказывает свойство 4. Так как подгруппа H минимальна, получаем, что $N = H$, что доказывает лемму.

Лемма 4. *Если H минимальна, то она разрешима.*

Согласно результатам гл. III, достаточно доказать, что H/H_0 разрешима. Пусть P — силовская подгруппа группы

H/H_0, B — ее прообраз в H, а N — его нормализатор. Снова применяя к N рассуждения предыдущей леммы (сопряженность борелевских подгрупп здесь заменяется сопряженностью силовских подгрупп), получаем, что $N = H$. Таким образом, любая силовская подгруппа группы H/H_0 является нормальным делителем; в этом случае группа H/H_0 есть произведение своих силовских подгрупп, следовательно, она нильпотентна и тем более разрешима.

Лемма 5. *Если* $\dim(k) \leqslant 1$ *и H минимальна, то H совпадает со своим коммутантом.*

Пусть H' — коммутант группы H. Определим прежде всего действия группы $G(\bar{k}/k)$ на H/H'. С этой целью для $h \in H$ и $s \in G(\bar{k}/k)$ положим

$$^{s'}h = a_s\, {}^s h a_s^{-1}.$$

Условие 4 показывает, что $^{s'}h$ принадлежит H; если, кроме того, $h \in H'$, то $^{s'}h \in H$. Таким образом, переходя к фактору, получаем автоморфизм $y \to {}^{s'}y$ группы H/H'. Воспользовавшись формулой 3, мы приходим к тому, что $^{st'}y = {}^{s'}({}^{t'}y)$. Это означает, что *$H/H'$ является $G(\bar{k}/k)$-группой.*

Обозначим через $\bar{h}_{s,t}$ образ $h_{s,t}$ в группе H/H'. Это 2-коцикл, что видно из тождества

$$a_{st} \cdot {}^s a_t^{-1} \cdot a_s^{-1} \cdot a_s \cdot {}^s a_t \cdot {}^{st} a_u \cdot {}^s a_{tu}^{-1} \cdot a_s^{-1} \cdot a_s \cdot {}^t a_{tu} \times$$
$$\times a_{stu}^{-1} \cdot a_{stu} \cdot {}^{st} a_u^{-1} \cdot a_{st}^{-1} = 1,$$

которое при переходе к H/H^1 дает равенство

$$\bar{h}_{s,t}^{-1} \cdot {}^{s'}\bar{h}_{t,u} \cdot \bar{h}_{s,tu} \cdot \bar{h}_{st,u}^{-1} = 1.$$

Однако известная теорема о структуре коммутативных алгебраических групп показывает, что группа $H/H(\bar{k})$ имеет композиционный ряд, факторы которого есть группы без кручения, а следовательно, делимы. Так как $\dim(k) \leqslant 1$, получаем, что $H^2(G(\bar{k}/k), H/H'(k)) = 0$, ср. гл. I, п. 3.1. Таким образом, коцикл $(\bar{h}_{s,t})$ является кограницей. Отсюда следует, что существует 1-коцепь (h_s) со значениями

в $H(\bar{k})$, такая, что

$$h_{st} = h_s^{-1} \cdot {}^{s'}h_t^{-1} \cdot h'_{s,t} \cdot h_{s,t}, \quad \text{где} \quad h'_{s,t} \in H'(\bar{k}).$$

Имеет место соотношение

$$^{ss'}h_t^{-1} = a_s {}^s h_t^{-1} \cdot a_s^{-1} \equiv h_s \cdot a_s {}^s h_t^{-1} a_s^{-1} h_s^{-1} \bmod H'(k).$$

Изменив в случае необходимости $h'_{s,t}$, можно записать

$$h_{s,t} = h_s^{-1} h_s a_s {}^s h_t^{-1} \cdot a_s^{-1} \cdot h_s^{-1} \cdot h'_{s,t} \cdot h_{s,t}.$$

Если положить $a'_s = h_s \cdot a_s$, предыдущая формула примет вид

$$a'_s \cdot {}^s a'_t = h'_{s,t} \cdot a'_{st}.$$

Система $\{H', (a'_s)\}$ удовлетворяет условиям 1, 2 и 3. Без труда проверяется также и условие 4. Поскольку H минимальна, получаем, что $H = H'$.

Конец доказательства. Если $\{H, (a_s)\}$ — минимальная система, то леммы 4 и 5 показывают, что $H = \{1\}$, а следовательно, (a_s) — коцикл, что доказывает предложение 7, а вместе с ним и теорему 3.

Упражнения. 1) В обозначениях доказательства леммы 5 показать, что на группе H/H' существует структура алгебраической k-группы, для которой структура соответствующего $G(\bar{k}/k)$-модуля на $H/H'(\bar{k})$ совпадает с определенной выше.

2) Показать, что теорема 3 остается справедливой, если заменить условие $\dim(k) \leqslant 1$ на следующее:

Стабилизатор точки x является унипотентной линейной группой. (Использовать, что $H^2(k, H) = 0$ для любой унипотентной коммутативной группы H.)

3) Предположим, что $\dim(k) \leqslant 1$ и характеристика $p \neq 2$.

Пусть f — невырожденная квадратичная форма от n переменных ($n \geqslant 2$). Используя теорему 3, показать, что для любой константы $c \neq 0$ уравнение $f(x) = c$ имеет решение в k. (Заметить, что схема решений этого уравнения является однородным пространством над унимодулярной ортогональной группой формы f, которая связна.) Заново

получить этот результат непосредственно, используя лишь тот факт, что когомологическая 2-размерность группы $G(\bar{k}/k)$ не больше 1.

§ 3. ПОЛЯ, РАЗМЕРНОСТЬ КОТОРЫХ НЕ ПРЕВОСХОДИТ 2

3.1. Формулировка гипотез

Напомним, что полупростая группа L называется *односвязной*, если любое проективное представление L получается проективизацией некоторого линейного представления L. Пусть T — максимальный тор в L; односвязность эквивалентна тому, что группа характеров $X(T)$ тора T совпадает с группой *весов*. (Ср. семинар Шевалле, 1956—1958.)

Гипотеза 2. *Пусть k — поле, когомологическая размерность группы Галуа $G(\bar{k}/k)$ которого не превосходит 2, и L — односвязная полупростая группа, определенная над k. Тогда $H^1(k, L) = 0$.*

Поскольку неизвестно, что следует считать „хорошим" определением полей, размерность которых не превосходит 2, сформулируем также следующие гипотезы:

Гипотеза 2′ (соответственно 2″). *Та же формулировка, что и у гипотезы 2, с заменой условия* $\mathrm{cd}(G(\bar{k}/k)) \leqslant 2$ *на условие* (C_2) (*соответственно* (C_2')), *п.* 4.5 *гл.* II.

Разумеется, из гипотезы 2″ следует гипотеза 2′ (поскольку $(C_2) \Rightarrow (C_2')$). Никакой импликации между гипотезами 2 и 2′ не известно.

Замечания. 1. Легко показать (воспользовавшись точной последовательностью неабелевых когомологий), что из гипотезы 2 следует гипотеза 1, п. 2.3.

2. М. Кнезер доказал (Кнезер [3]) следующий частный случай гипотезы 2:

Если k — конечное расширение поля $\mathbf{Q}_p$ и L — полупростая односвязная группа, определенная над k, то $H^1(k, L) = 0$.

3. Г. Хардер доказал гипотезу 2 и гипотезы п. 3.3 (см. ниже) в случае, когда k — вполне мнимое поле алге-

брических чисел, а L не содержит сомножителей типа $\mathbf{E}_8$ (не опубликовано).

3.2. Примеры

(а) *Группа* $\mathbf{SL}(D)$.

Пусть D — тело с центром k размерности n^2 над k. Пусть $\mathbf{G}_m(D)$ — алгебраическая группа над k, рациональные точки которой над расширением k'/k совпадают с группой обратимых элементов $D \underset{k}{\otimes} k'$; ясно, что это k-форма группы $\mathbf{GL}_n$.

Приведенная норма N_{red}[1]) определяет сюръективный гомоморфизм

$$N_{\mathrm{red}}: \mathbf{G}_m(D) \to \mathbf{G}_m.$$

Обозначим через $\mathbf{SL}(D)$ ядро гомоморфизма N_{red}. Это k-форма группы $\mathbf{SL}_n$, а следовательно, односвязная полупростая группа. Когомологии этой группы определяются с помощью точной последовательности

$$H^0(k, \mathbf{G}_m(D)) \to H^0(k, \mathbf{G}_m) \to$$
$$\to H^1(k, \mathbf{SL}(D)) \to H^1(k, \mathbf{G}_m(D)).$$

Первые две группы равны здесь соответственно D^* и k^*. Легко доказывается (с помощью „сумм Пуанкаре“), что $H^1(k, \mathbf{G}_m(D)) = 0$. Отсюда следует, что $H^1(k, \mathbf{SL}(D)) = 0$ *в том и только том случае, когда гомоморфизм* N_{red}: $D^* \to k^*$ *сюръективен*, что выполняется (по определению), если k удовлетворяет условию (C_2').

(б) *Группа* $\mathbf{Spin}_n$.

Пусть f — невырожденная квадратичная форма от n переменных; предположим, что характеристика k отлична от 2, и пусть $\mathbf{SO}_n$ — соответствующая унимодулярная ортогональная группа. Эта группа (в предположении, что $n \geqslant 3$) полупроста. Ее универсальное накрытие совпадает с группой $\mathbf{Spin}_n$. Имеет место точная последовательность

$$0 \to \mu_2 \to \mathbf{Spin}_n \to \mathbf{SO}_n \to 0, \quad \text{где} \quad \mu_2 = \{\pm 1\},$$

---

[1]) Ср. Бурбаки [4*], гл. 8, § 12, п. 3. — *Прим. перев.*

из которой получаем точную последовательность групп когомологий:

$$\mathbf{Spin}_n(k) \to \mathbf{SO}_n(k) \xrightarrow{\delta} k^*/k^{*2} \to H^1(k, \mathbf{Spin}_n) \to$$
$$\to H^1(k, \mathbf{SO}_n) \xrightarrow{\Delta} H^2(k, \mu_2).$$

Группа $H^2(k, \mu_2)$ отождествляется с подгруппой $\mathrm{Br}(k)_2$ группы Брауэра $\mathrm{Br}(k)$, образованной элементами, для которых $2x = 0$. Гомоморфизм δ: $\mathbf{SO}_n(k) \to k^*/k^{*2}$ — *спинорная норма* [1]), отображение Δ: $H^1(k, \mathbf{SO}_n) \to \mathrm{Br}(k)_2$ непосредственно связано с *инвариантом Витта* квадратичной формы (относительно подробностей см. Спрингер [1], стр. 241, а также Дельзант [1], стр. 1366). Заметим, что группу $H^1(k, \mathbf{SO}_n)$ можно отождествить с множеством классов квадратичных форм от n переменных, имеющих тот же дискриминант, что и f. Выписанная точная последовательность дает следующий результат:

Для того чтобы $H^1(k, \mathbf{Spin}_n) = 0$, необходимо и достаточно, чтобы выполнялись следующие два условия:

(i) *отображение спинорной нормы δ: $\mathbf{SO}_n(k) \to k^*/k^{*2}$ сюръективно;*

(ii) *каждая квадратичная форма, имеющая тот же дискриминант и инвариант Витта, что и f, ей эквивалентна.*

Можно показать, что эти условия выполнены, если каждая квадратичная форма от 5 переменных над k представляет 0 (ср. Витт [1]), в частности, следовательно, когда k удовлетворяет условию (C_2'). Это доказывает тем самым другой частный случай гипотезы 2″.

3.3. Смежные вопросы

(а) Пусть L — полупростая группа, C — подгруппа группы L, содержащаяся в ее центре. В гл. I, п. 5.7, было определено каноническое отображение

$$\Delta: H^1(k, L/C) \to H^2(k, C).$$

Сюръективно ли это отображение, если k удовлетворяет одному из условий гипотез 2, 2′, 2″? Наиболее интересный случай получается, когда L односвязна, в этом случае

---

[1]) Ср. Бурбаки [4*], гл. 9, § 9, п. 5. — *Прим. перев.*

отображение Δ инъективно (при условии, что справедливы рассматриваемые гипотезы).

(б) Предположим, что k есть p-адическое поле (конечное расширение поля $\mathbf{Q}_p$). Полупростая группа L над k называется *анизотропной*, если она не содержит отличных от 1 унипотентных элементов, рациональных над k. Согласно одной теореме Годемана, это эквивалентно тому, что аналитическая группа $L(k)$ *компактна*. Верно ли, что любая простая анизотропная группа имеет тип $\mathbf{A}_n$? Здесь также можно попытаться проверить отдельные случаи, однако случай $\mathbf{E}_8$ до сих пор не поддается (см. последнее замечание в п. 3.1).

§ 4. ТЕОРЕМЫ КОНЕЧНОСТИ

4.1. Условие (F)

Предложение 8. *Пусть G — проконечная группа. Следующие три условия эквивалентны*:

(а) *группа G имеет только конечное число открытых подгрупп индекса n для любого целого числа n*;

(а′) *то же самое утверждение для открытых нормальных делителей*;

(б) *для любой конечной G-группы A* (ср. гл. I, п. 5.1) *множество $H^1(G, A)$ конечно.*

Если H — открытая подгруппа в G индекса n, то пересечение H' подгрупп, сопряженных с H, является открытым нормальным делителем G индекса, не превосходящего $n!$ (Действительно, факторгруппа G/H' изоморфна подгруппе группы перестановок группы G/H.) Отсюда легко следует эквивалентность условий (а) и (а′).

Покажем, что (а)$\Rightarrow$(б). Пусть n — порядок конечной G-группы A и H — открытый нормальный делитель группы G, тривиально действующий на A. В силу условия (а) существует лишь конечное число открытых подгрупп H индекса меньшего или равного n. Их пересечение H' есть открытый нормальный делитель группы G. Всякий непрерывный гомоморфизм $f\colon H \to A$ тривиален на H'. Отсюда следует, что композиция

$$H^1(G, A) \to H^1(H, A) \to H^1(H', A)$$

11 Зак. 1202

тривиальна. Таким образом (ср. точную последовательность гл. I, п. 5.8), группа $H^1(G, A)$ отождествляется с $H^1(G/H', A)$, которая, очевидно, конечна.

Покажем, что (б) $\Rightarrow$ (а). Для этого надо доказать, что для любого n существует только конечное число гомоморфизмов группы G в симметрическую группу $\mathbf{S}_n$. Это следует немедленно из конечности $H^1(G, \mathbf{S}_n)$, где G тривиально действует на $\mathbf{S}_n$.

Каждая проконечная группа G, удовлетворяющая условиям предложения 8, будет называться группой „типа (F)“.

Предложение 9. *Каждая проконечная группа G, топологически порожденная конечным числом элементов, имеет тип* (F).

Действительно, существует только конечное число гомоморфизмов G в конечную группу (поскольку они определяются своими значениями на топологических образующих G).

Следствие. *Про-p-группа имеет тип* (F) *тогда и только тогда, когда она топологически конечно порождена.*

Это следует из двух предыдущих предложений и предложения 25 гл. II.

Упражнения. 1) Пусть G — проконечная группа типа (F) и f: $G \to G$ — *сюръективный* гомоморфизм G на себя. Показать, что f — изоморфизм. [Пусть X_n — множество открытых подгрупп в G данного индекса n. Если $H \in X_n$, то $f^{-1}(H) \in X_n$ и, следовательно, f определяет инъекцию f_n: $X_n \to X_n$. Так как X_n — конечные множества, то отображение f_n является биекцией. Отсюда следует, что ядро N отображения f содержится во всех открытых подгруппах G, а следовательно, совпадает с $\{1\}$.]

2) Пусть (N_p), $p = 2, 3, \ldots,$ — неограниченное семейство целых положительных чисел, занумерованных простыми числами. Пусть G_p есть N_p-я степень группы $\mathbf{Z}_p$, а G — произведение всех G_p. Показать, что группа G имеет тип (F), однако не порождается конечным числом элементов.

4.2. Поля типа (F)

Пусть k — поле. Будем говорить, что k имеет *тип* (F), если k совершенно и его группа Галуа $G(\bar{k}/k)$ имеет тип (F) в смысле предыдущего определения. Это последнее условие сводится к тому, что для любого целого числа n существует только конечное число подрасширений $\bar{k}$ (соответственно подрасширений Галуа) степени n над k.

Примеры полей типа (F). (а) Поле $\mathbf{R}$ *вещественных чисел.*

(б) *Конечное* поле. (Действительно, такое поле имеет единственное расширение данной степени, более того, его группа Галуа изоморфна $\hat{\mathbf{Z}}$, а следовательно, топологически порождена одним элементом.)

(в) Поле $C((T))$ *формальных степенных рядов* от одной переменной над алгебраически замкнутым полем C нулевой характеристики. [То же рассуждение, что и в предыдущем случае; заметить, что, согласно теореме Пюизе (ср. [CL], стр. 76)[1]), все расширения $C((T))$ имеют вид $C\left(\left(T^{\frac{1}{n}}\right)\right)$.]

(г) *p-адическое* поле (конечное расширение поля $\mathbf{Q}_p$). Это следует из хорошо известного результата, который можно доказать, например, следующим образом: каждое конечное расширение поля k является чисто разветвленным расширением неразветвленного расширения k. Так как существует лишь единственное неразветвленное расширение данной степени, *все сводится к чисто разветвленному случаю.* Однако такое расширение задается „уравнением Эйзенштейна" $T^n + a_1T^{n-1} + \ldots + a_n = 0$, где a_i — целые элементы поля k, а a_n — униформизирующая. Множество таких уравнений образует *компактное* пространство относительно топологии сходимости коэффициентов; с другой стороны, известно, что близкие уравнения определяют изоморфные расширения (это следствие „леммы Краснера",

---

[1]) Ср. также К. Шевалле [5*]. — *Прим. перев.*

ср., например, [CL], стр. 40, упр. 1 и 2)[1]). Отсюда получается нужная нам конечность.

На самом деле известны гораздо более точные утверждения.

(i) Краснер явно вычислил число расширений данного поля k степени n (см. по этому поводу Краснер [1])[2]).

(ii) Ивасава доказал, что группа Галуа $G(\bar{k}/k)$ топологически порождается конечным числом элементов, ср. Ивасава [2] (этот результат у него явно не сформулирован, но легко следует из теоремы 3, стр. 468).

Упражнение. Пусть k — совершенное поле. Предположим, что для любого целого числа n и любого конечного расширения K поля k факторгруппа K^*/K^{*n} конечна. Показать, что существует только конечное число *разрешимых* расширений Галуа данного поля k данной степени, взаимно простой с характеристикой. Как применить это к p-адическому полю?

4.3. Конечность когомологий линейных групп

Теорема 4. *Пусть k — поле типа* (F), *а L — алгебраическая линейная группа, определенная над k. Множество $H^1(k, L)$ конечно.*

Доказывается в несколько шагов.

(i) Группа L *конечна* (т. е. размерности 0).

В этом случае множество $L(\bar{k})$ рациональных над $\bar{k}$ точек группы L является конечной $G(\bar{k}/k)$-группой, к которой можно применить предложение 8. Отсюда следует конечность множества $H^1(k, L) = H^1(G(\bar{k}/k), L(\bar{k}))$.

(ii) Группа L *связна и разрешима.*

Применяя следствие 3 к предложению 39 гл. I, получаем, что все сводится к случаю, когда L — унипотентная группа или тор. В первом случае $H^1(k, L) = 0$, ср. предложение 6. Предположим теперь, что L — тор. Тогда существует конечное расширение Галуа k'/k, такое, что L

---

[1]) Ср. также Ленг [4*], гл. 2, § 2, предложение 4. — *Прим. перев.*

[2]) Подробное изложение работ Краснера можно найти в его статье [2*]. — *Прим. перев.*

k'-изоморфна произведению мультипликативных групп $\mathbf{G}_m$. Так как $H^1(k', \mathbf{G}_m)=0$, получаем, что $H^1(k, L)=0$, а, следовательно, группу $H^1(k, L)$ можно отождествить с $H^1(k'/k, L)$. В частности, если $n=[k': k]$, то $nx=0$ для всех $x \in H^1(k, L)$. Рассмотрим теперь точную последовательность

$$0 \to L_n \to L \xrightarrow{n} L \to 0$$

и соответствующую когомологическую последовательность. Мы видим, что группа $H^1(k, L_n)$ отображается на ядро отображения $H^1(k, L) \xrightarrow{n} H^1(k, L)$, т. е. на всю группу $H^1(k, L)$. Поскольку группа L_n конечна, случай (i) показывает, что $H^1(k, L_n)$ конечна, а следовательно, конечна и $H^1(k, L)$.

(iii) *Общий случай.*

Воспользуемся следующим результатом, принадлежащим Спрингеру:

Лемма 6. *Пусть C — картановская подгруппа линейной группы L, а N — нормализатор C в L. Тогда каноническое отображение $H^1(k, N) \to H^1(k, L)$ сюръективно.*

(Этот результат верен для любого совершенного поля k.) Пусть $x \in H^1(k, L)$, а c — коцикл, представляющий x. Пусть ${}_cL$ — группа, полученная скручиванием L с помощью c. Согласно одной теореме Розенлихта, группа ${}_cL$ содержит картановскую подгруппу C', определенную над k; при расширении основного поля до $\bar{k}$ группы C и C' становятся сопряженными. В силу леммы 1 из п. 2.2 отсюда следует, что x принадлежит образу $H^1(k, N)$ в группе $H^1(k, L)$, что и доказывает лемму.

Вернемся теперь к доказательству теоремы 4. Пусть C — картановская подгруппа группы L, определенная над k, и N — ее нормализатор. По предыдущей лемме достаточно доказать, что группа $H^1(k, N)$ конечна. Факторгруппа N/c конечна; в силу (i) группа $H^1(k, N/C)$ также конечна. С другой стороны, для любого коцикла c со значениями в N скрученная группа ${}_cC$ связна и разрешима, таким образом в силу результата пункта (iii) $H^1(k, {}_cC)$ конечна. Применяя теперь следствие 3 к предложению 39, гл. I, получаем, что группа $H^1(k, N)$ конечна, что и требовалось доказать.

Следствие. *Пусть k — поле типа* (F).

(а) *Существует только конечное число k-форм полупростой группы, определенной над k (с точностью до изоморфизма).*

(б) *То же самое относительно k-форм пары* (V, x), *где V — векторное пространство, а x — тензор* (ср. п. 1.1).

Это следует из того, что в обоих случаях группа автоморфизмов рассматриваемой структуры является алгебраической линейной группой.

Замечания. 1. Если k — поле нулевой характеристики и типа (F), то можно показать, что у любой алгебраической *линейной* группы имеется только конечное число k-форм; для этого надо распространить теорему 4 на некоторые неалгебраические группы, которые являются расширениями дискретных групп „арифметического типа" с помощью линейной группы; относительно подробностей см. Борель, Серр [1].

2. Пусть k_0 — конечное поле, $k = k_0((T))$. Теорема 4 не применима к k (уже потому, что k несовершенно — можно даже показать, что группа $H^1(k, \mathbf{Z}/p\mathbf{Z})$ бесконечна). Тем не менее возможно, что, когда L *редуктивна*[1]), в частности полупроста, группа $H^1(k, L)$ конечна.

4.4. Конечность орбит

Теорема 5. *Пусть k — поле типа* (F), *G — алгебраическая группа над k, а V — однородное пространство группы G. Фактормножество $V(k)$ по отношению эквивалентности, определяемому группой $G(k)$, конечно.*

Пространство V является объединением конечного числа орбит связной компоненты единицы группы G; это позволяет свести все *к случаю, когда G связна.* Если $V(k) = \varnothing$, то нечего доказывать. В противном случае, пусть $v \in V(k)$ и H — стабилизатор v. Каноническое отображение $G/H \to V$ определяет биекцию множества $(G/H)(k)$ на $V(k)$. След-

[1]) Алгебраическая k-группа G называется редуктивной, если ее унипотентный радикал (т. е. максимальный связный унипотентный нормальный делитель G) сводится к единице. — *Прим. перев.*

ствие 1 к предложению 36 гл. I показывает, что фактор $(G/H)(k)$ по $G(k)$ можно отождествить с ядром канонического отображения $\alpha: H^1(k, H) \to H^1(k, G)$. Таким образом, достаточно доказать, что это отображение *собственно*, т. е. что α^{-1} преобразует конечное множество в конечное.

Пусть L — максимальная связная линейная подгруппа в G, $M = L \cap H$, $A = G/L$, $B = H/M$. Согласно теореме Шевалле, A — абелево многообразие, а B инъективно погружается в A. Имеет место коммутативная диаграмма

$$\begin{array}{ccc} H^1(k, H) & \xrightarrow{\alpha} & H^1(k, G) \\ \downarrow{\gamma} & & \downarrow{\beta} \\ H^1(k, B) & \xrightarrow{\delta} & H^1(k, A) \end{array}$$

Поскольку группа M линейна, теорема 4 (вместе с предложением 39 гл. I) показывает, что отображение γ собственно. С другой стороны, теорема о „полной приводимости“ абелева многообразия[1]) показывает, что существует абелево многообразие B' той же размерности, что и B, и гомоморфизм $A \to B'$, такой, что композиция $B \to A \to B'$ сюръективна; кроме того, многообразие B' и морфизм $A \to B'$ можно определить над k. Так как ядро отображения $B \to B'$ конечно, используемое выше рассуждение показывает, что композиция $H^1(k, B) \to H^1(k, A) \to \to H^1(k, B')$ собственна. Отсюда следует, что отображение δ собственно, а, следовательно, собственно и отображение $\delta \circ \gamma = \beta \circ \alpha$. Таким образом получается нужное нам свойство морфизма α, что и требовалось доказать.

Следствие 1. *Пусть k — поле типа* (F), *а G — линейная алгебраическая группа над k. Максимальные торы (соответственно картановские подгруппы) группы G образуют конечное число классов (относительно сопряжения элементами из G/k).*

Пусть T — максимальный тор (соответственно картановская подгруппа) группы G, определенный над k (если такого нет, то нечего доказывать); пусть H — его нормализатор в G. Поскольку все максимальные торы (соответ-

[1]) Ср. М. Бальдассари [1*], стр. 149. — *Прим. перев.*

ственно картановские подгруппы) сопряжены над $\bar{k}$, то они биективно соответствуют точкам однородного пространства G/H; те из них, которые определены над k, соответствуют рациональным над k точкам G/H; в силу теоремы 5 они распределяются в конечное число классов по модулю $G(k)$, откуда получаем искомый результат.

Следствие 2. *Пусть k — поле нулевой характеристики типа* (F), *а G — полупростая группа над k. Унипотентные элементы из $G(k)$ образуют конечное число классов (относительно сопряжения элементами из $G(k)$).*

Доказательство такое же, как и для следствия 1, используется тот факт (доказанный Костантом), что унипотентные элементы в $G(\bar{k})$ образуют конечное число классов.

Упражнения. Поле k здесь совершенное поле типа (F).

1) Пусть $f: G \to G'$ — гомоморфизм алгебраических групп. Предположим, что ядро f является линейной группой. Показать, что соответствующее отображение $H^1(k, G) \to H^1(k, G')$ собственно.

2) Пусть G — алгебраическая группа, а K — конечное расширение поля k. Показать, что отображение $H^1(k, G) \to$ $\to H^1(K, G)$ собственное. [Применить результат упр. 1 к группе $G' = R_{K/k}(G)$.]

4.5. Вещественный случай

Разумеется, результаты предыдущих пунктов можно применить к полю $\mathbf{R}$. Впрочем, некоторые из них проще получить с помощью топологических рассуждений. Так, например, теорема 5 следует из того факта (доказанного Уитнеем), что всякое вещественное алгебраическое многообразие имеет только конечное число связных компонент. Мы покажем, что для некоторых групп можно пойти дальше и явно вычислить группу H^1.

Начнем с *компактной группы Ли K*. Пусть R — алгебра непрерывных функций на K, являющихся линейными комбинациями коэффициентов матричных представлений (комплексных) группы K. Обозначая через R_0 подалгебру вещественных функций, получаем, что $R = R_0 \otimes_{\mathbf{R}} \mathbf{C}$. Известно (ср., например, Шевалле [4], гл. 6), что R_0 — афин-

ная алгебра некоторой алгебраической $\mathbf{R}$-группы L. Группа $L(\mathbf{R})$ вещественных точек L отождествляется с K. Группа $L(\mathbf{C})$ называется *комплексификацией* группы K. Очевидно, на $L(\mathbf{C})$ действует группа Галуа $\mathfrak{g}=G(\mathbf{C}/\mathbf{R})$.

Теорема 6. *Каноническое отображение* ε: $H^1(\mathfrak{g}, K)\to H^1(\mathfrak{g}, L(\mathbf{C}))$ *биективно.*

[Так как $\mathfrak{g}$ действует тривиально на K, $H^1(\mathfrak{g}, K)$ есть множество классов сопряженных элементов x в K, для которых $x^2=1$.]

Группа $\mathfrak{g}$ действует на алгебре Ли $L(\mathbf{C})$; инвариантные элементы образуют алгебру Ли $\mathfrak{k}$ группы K, дополнение $\mathfrak{p}$ к которой образовано антиинвариантными элементами. Экспоненциальное отображение определяет вещественный аналитический изоморфизм подалгебры $\mathfrak{p}$ на замкнутое подмногообразие P группы $L(\mathbf{C})$; ясно, что $xPx^{-1}=P$ для всех $x\in X$; кроме того (Шевалле [4]), каждый элемент $z\in L(\mathbf{C})$ можно однозначно записать в виде $z=xp$, где $x\in K$ и $p\in P$.

Напомнив эти результаты, покажем, что отображение ε *сюръективно.* 1-коцикл группы $\mathfrak{g}$ в $L(\mathbf{C})$ отождествляется с элементом $z\in L(\mathbf{C})$, таким, что $z\bar{z}=1$. Если записать z в виде xp, где $x\in K$, а $p\in P$, то получим, что $xpx\bar{p}^{-1}=1$ (так как $\bar{p}=p^{-1}$), откуда $p=x^2\cdot x^{-1}px$. Но $x^{-1}px$ принадлежит P и однозначность разложения $L(\mathbf{C})=K\cdot P$ показывает, что $x^2=1$ и $x^{-1}px=p$. Пусть P_x обозначает подмножество P, состоящее из элементов, коммутирующих с x; легко видеть, что x совпадает с образом векторного подпространства $\mathfrak{p}$ при экспоненциальном отображении. Отсюда следует, что p можно записать в виде $p=q^2$, где $q\in P_X$. Это показывает, что $z=qx\bar{q}$ и, так как $\bar{q}=q^{-1}$, получаем, что коцикл z когомологичен коциклу x со значениями в K.

Покажем теперь, что отображение $H^1(\mathfrak{g}, K)\to H^1(\mathfrak{g}, L(\mathbf{C}))$ *инъективно.* Пусть x, $x'\in K$ — два таких элемента, что $x^2=1$ и $x'^2=1$, и предположим, что они когомологичны в $L(\mathbf{C})$, т. е. что существует такой элемент $z\in L(\mathbf{C})$, что $x'=z^{-1}x\bar{z}$. Представим z в виде $z=yp$, где $y\in K$ и $p\in P$. Тогда

$$x'=p^{-1}y^{-1}xyp^{-1},$$

откуда следует, что

$$x' \cdot x'^{-1} pX' = y^{-1}xy \cdot p^{-1}.$$

Воспользовавшись снова однозначностью разложения $L(\mathbf{C}) = P \cdot K$, получаем, что $x' = y^{-1}xy$, а это означает, что x и x' сопряжены в K, и тем самым завершает доказательство.

Примеры. (а) Предположим, что группа K *связна*, и пусть T — один из ее максимальных торов. Обозначим через T_2 множество элементов $t \in T$, таких, что $t^2 = 1$. Известно, что любой элемент $x \in K$, для которого $x^2 = 1$, сопряжен элементу $t \in T_2$; кроме того, $t, t' \in T_2$ сопряжены в K в том и только том случае, когда они преобразуются элементом из *группы Вейля* в один и тот же элемент[1]). Таким образом, теорема 6 показывает, что группа $H^1(\mathbf{R}, L) = H^1(\mathfrak{g}, L(\mathbf{C}))$ *отождествляется с фактормножеством* T_2/W.

(б) Возьмем в качестве K *группу автоморфизмов* связной полупростой компактной группы S. Пусть A (соответственно L)—алгебраическая группа, ассоциированная с K (соответственно S). Классический результат показывает, что A является *группой автоморфизмов группы* L. Таким образом, элементы группы $H^1(\mathbf{R}, A)$ соответствуют *вещественным формам группы* L, и теорема 6 заново дает классификацию этих форм с помощью классов „инволюций“ группы S (принадлежащую Эли Картану).

4.6. Поля алгебраических чисел (теорема Бореля)

Пусть k — поле алгебраических чисел. Ясно, что k не является *полем типа* (F). Тем не менее имеет место следующая теорема конечности.

Теорема 7. *Пусть L — алгебраическая линейная группа, определенная над k, а S — конечное множество*

---

[1]) Пусть G — алгебраическая аффинная группа, T — ее максимальный тор, N — его нормализатор в G, а Z — его централизатор. Факторгруппа $W = N/Z$ конечна и называется группой Вейля группы G. Так как все максимальные торы группы G сопряжены, это определение не зависит от выбранного тора T. — *Прим. перев.*

точек поля k. Каноническое отображение

$$\omega_S: H^1(k, L) \to \prod_{v \notin S} (H^1(k_v, L)$$

собственно.

Поскольку группы $H^1(k_v, L)$ *конечны* (ср. теорему 4), множество S можно как угодно менять, и в частности можно считать, что $S = \varnothing$ (в этом случае вместо ω_S мы будем писать ω). Кроме того, *скручивая* L, приходим к выводу, что достаточно показать, что ядро ω конечно; другими словами,

Теорема 7. *Существует только конечное число локально тривиальных элементов группы* $H^1(k, L)$.

В случае, когда L — связная редуктивная группа, в этой форме теорема была доказана Борелем [2], см. также доклад Годемана на семинаре Бурбаки в июне 1963 г. Случай связной линейной группы немедленно сводится к этому случаю. Несколько труднее избавиться от условия связности, относительно этого я отсылаю к уже цитированной статье Бореля — Серра.

4.7. Контрпример к „принципу Хассе"

Сохраним обозначения п. 4.6. Существуют важные примеры, когда отображение

$$\omega: H'(k, L) \to \prod_{v} H'(k_v, L)$$

инъективно; например, когда L — проективная или ортогональная группа. Естественно задать вопрос, распространяется ли „принцип Хассе" на все полупростые группы. Мы покажем, что это не так.

Лемма 7. *Существует конечный $G(\bar{k}/k)$-модуль A, для которого каноническое отображение группы $H^1(k, A)$ в $\prod_{v} H^1(k_v, A)$ неинъективно.*

Начнем с того, что возьмем конечное расширение Галуа K/k, группа Галуа G которого обладает следующим свойством:

Наименьшее общее кратное порядков групп разложения точек v поля k строго меньше порядка n группы G.

[Пример. $k = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{13}, \sqrt{17})$; здесь группа Галуа типа (2,2), ее группы разложения циклические второго порядка или единичные. Аналогичные примеры существуют над любым числовым полем.]

Пусть $E = \mathbf{Z}/n\mathbf{Z}[G]$ — групповая алгебра группы G над кольцом $\mathbf{Z}/n\mathbf{Z}$, а A — ядро пополняющего гомоморфизма $E \to \mathbf{Z}/n\mathbf{Z}$. Так как когомологии группы E тривиальны, точная когомологическая последовательность показывает, что $H^1(G, A) = Z/nZ$. Обозначим через x образующую группы $H^1(G, A)$, а через q — наименьшее общее кратное порядков групп разложения G_v, и пусть $y = qx$. Очевидно, $y \neq 0$; с другой стороны, поскольку каждый элемент группы $H^1(G_v, A)$ аннулируется q, образ y в $H^1(G_v, A)$ нулевой. Поскольку группа $H^1(G, A)$ отождествляется с подгруппой $H^1(k, A)$, мы построили тем самым ненулевой элемент $y \in H^1(k, A)$, все локальные образы которого нулевые.

Лемма 8. *Существует конечный $G(\bar{k}/k)$-модуль B, для которого каноническое отображение $H^2(k, B)$ в $\prod_v H^2(k_v, B)$ неинъективно.*

Это значительно менее тривиально. Можно действовать двумя способами:

1) Начнем с построения конечного $G(\bar{k}/k)$-модуля A, удовлетворяющего условию леммы 7. Положим затем

$$B = A' = \mathrm{Hom}(A, \bar{k}^*).$$

По теореме двойственности Тейта ядра отображений

$$H^1(k, A) \to \prod_v H^1(k_v, A) \quad \text{и} \quad H^2(k, B) \to \prod_v H^2(k_v, B)$$

двойственны друг другу. Так как первое ядро отлично от нуля, второе также ненулевое.

2) Явная конструкция. Возьмем в качестве B некоторое расширение

$$0 \to \mu_n \to B \to \mathbf{Z}/n\mathbf{Z} \to 0,$$

где μ_n обозначает группу корней n-й степени из 1. Выберем модуль B таким, чтобы, как абелева группа, он был прямой суммой $\mu_n \oplus \mathbf{Z}/n\mathbf{Z}$; в этом случае его структура

$G(\bar{k}/k)$-модуля определяется элементом группы

$$H^1(k, \operatorname{Hom}(\mathbf{Z}/n\mathbf{Z}, \mu_n)) = H^1(k, \mu_n) = k^*/k^{*^n}.$$

В качестве интересующего нас элемента группы $H^2(k, B)$ выберем канонический образ $\bar{x}$ некоторого элемента $x \in H^2(k, \mu_n)$, который можно отождествить с элементом группы Брауэра, порядок которого делит n. Но такой элемент задается *локальными инвариантами* $x_v \in \left(\frac{1}{n}\mathbf{Z}\right)/\mathbf{Z}$, удовлетворяющими обычным условиям ($\sum x_v = 0$, $2x_v = 0$, если v — вещественная точка и $x_v = 0$, если точка v комплексная). Мы хотим устроить так, чтобы элемент $\bar{x}$ был отличен от нуля, а локально был нулевым. Первое условие сводится к тому, что x не принадлежит образу гомоморфизма d: $H^1(k, \mathbf{Z}/n\mathbf{Z}) \to H^2(k, \mu_n)$. Это отображение легко вычислить явно; прежде всего группа $H^1(k, \mathbf{Z}/n\mathbf{Z})$ совпадает с группой гомоморфизмов χ: $G(\bar{k}/k) \to \left(\frac{1}{n}\mathbf{Z}\right)/\mathbf{Z}$. Согласно теории полей классов, χ отождествляется с гомоморфизмом группы классов иделей поля k в $\left(\frac{1}{n}\mathbf{Z}\right)/\mathbf{Z}$; обозначим через (χ_v) локальные компоненты χ. Без труда проверяется, что кограница $d\chi$ элемента χ принадлежит группе $H^2(k, \mu_n)$ и ее локальные компоненты $(d\chi)_v$ равны $\chi_v(y)$. Таким образом, первое условие, накладываемое на x, эквивалентно следующему:

(а) *Не существует характера* $\chi \in H^1(k, \mathbf{Z}/n\mathbf{Z})$, *для которого* $x_v = \chi_v(y)$ *для всех* v.

Условие, что элемент $\bar{x}$ — локально нулевой, означает, что

(б) *Для любой точки* v *существует* $\varphi_v \in H^1(k_v, \mathbf{Z}/n\mathbf{Z})$, *для которого* $x_v = \varphi_v(y)$.

Числовой пример: $k = \mathbf{Q}$, $y = 14$, $n = 8$, $\chi_v = 0$ для $v \neq 2, 17$ и $x_2 = -x_{17} = 1/8$.

Надо проверить условия (а) и (б).

Проверка (а). Предположим, что существует глобальный характер χ, такой, что $\chi_v(14) = x_v$. Рассмотрим сумму $\sum \chi_v(16)$ (которая должна быть нулевой, поскольку χ аннулируется на главных иделях). Хорошо известно, что число 16 есть 8-я степень в локальных полях $\mathbf{Q}_p$, $p \neq 2$

(ср. Артин, Тейт [1], стр. 96), таким образом, $\chi_v(16)=0$ для $v\neq 2$. С другой стороны, $14^4\equiv 16 \mod \mathbf{Q}_2^{*8}$ (для этого надо показать, что $7^4\in\mathbf{Q}_2^{*8}$, а это следует из того, что —7 есть 2-адический квадрат). Отсюда получаем, что $\chi_2(16)=4\chi_2(14)=1/2$ и сумма всех $\chi_v(16)$ отлична от нуля. Это и дает искомое противоречие.

Проверка (б). Для $v\neq 2,17$ положим $\varphi_v=0$. Для $v=2$ определим характер группы $\mathbf{Q}_2^*$ формулой $\varphi_2(\alpha)=$ $=w(\alpha)/8$, где $w(\alpha)$ — значение нормирования α; очевидно, что $\varphi_2(y)=\varphi_2(14)=1/8$. Для $v=17$ заметим, что мультипликативная группа $(\mathbf{Z}/17\mathbf{Z})^*$ — циклическая порядка 16 и имеет в качестве образующей $y=14$ (достаточно проверить, что $14^8\equiv -1 \mod 17$ или что $2^8\equiv 1 \mod 17$ и $7^8\equiv(-2)^4\equiv -1 \mod 17$). Таким образом, существует характер φ_{17} группы 17-адических единиц порядка 8, имеющий на y значение $-1/8$; его можно продолжить, все равно каким способом, до характера порядка 8 группы $\mathbf{Q}_{17}^*$, что заканчивает проверку условия (б).

[Этот пример мне указал Тейт; пример, которым я пользовался сначала, был сложнее.]

Лемма 9. *Пусть B — конечный $G(\bar{k}/k)$-модуль и $x\in H^2(k, B)$. Существует полупростая группа S над k, центр Z которой содержит B и которая обладает следующими двумя свойствами*:

(а) *Элемент x принадлежит образу гомоморфизма d: $H^1(k, Z/B)\to H^2(k, B)$.*

(б) $H^1(k_v, S)=0$ *для любой точки v поля k.*

Пусть n — целое число, $n\geqslant 1$, такое, что $nB=0$. Возьмем достаточно большое конечное расширение Галуа K/k, для которого выполняются следующие три условия: (i) B есть $G(k/k)$-модуль, (ii) x получается из элемента $x'\in H^2(G(K/k), B)$, (iii) поле K содержит корни n-й степени из 1. Обозначим через $B'=\mathrm{Hom}(B, \mathbf{Q}/\mathbf{Z})$ двойственный к B модуль; очевидно, можно записать B' как фактормодуль свободного модуля над кольцом $\mathbf{Z}/n\mathbf{Z}$ $[G(K/k)]$. По двойственности *B можно погрузить в свободный модуль Z ранга q над кольцом* $\mathbf{Z}/n\mathbf{Z}[G(K/k)]$. Так как Z свободен, $H^2(G(K/k), Z)=0$ и существует такой элемент $y\in H^1(G(K/k), \mathbf{Z}/B)$, что $dy'=x'$; элемент y' определяет элемент $y\in H^1(k, Z/B)$, кроме того, ясно, что $dy=x$.

Итак, все сводится к отысканию полупростой группы S с центром Z, удовлетворяющей условию (б) леммы.

Будем исходить из группы $L = \mathbf{SL}_n \times \ldots \times \mathbf{SL}_n$ (q сомножителей). Если рассматривать L как алгебраическую группу над K, то центр L изоморфен $\mathbf{Z}/n\mathbf{Z} \times \ldots \times \mathbf{Z}/n\mathbf{Z}$ (все его элементы рациональны над K, так как мы заранее предположили, что K содержит корни n-й степени из 1). Возьмем за S группу $P_{K/k}(L)$, полученную из L ограничением основного поля K до k. Центр группы S изоморфен (как $G(\bar{k}/k)$-модуль) прямой сумме q экземпляров групп

$$R_{(K/k)}(\mathbf{Z}/n\mathbf{Z}) = \mathbf{Z}/n\mathbf{Z}\,[G(K/k)],$$

а следовательно, его можно отождествить с введенным выше модулем Z. Итак, остается проверить условие (б). Однако легко видеть, что группа $S \underset{k}{\otimes} k_v$ изоморфна произведению групп $R_{K_w/k_v}(L)$, где w принадлежит множеству точек поля K, продолжающих v (ср. Вейль [4]); таким образом, $H^1(k_v, S) = \prod_{w \mid v} H^1(K_w, L) = 0$, поскольку когомологии группы $\mathbf{SL}_n$ тривиальны. Теперь можно построить нужный пример.

Теорема 8. *Существует полупростая алгебраическая группа G над k и элемент $t \in H^1(k, G)$, для которого:*

(а) $t \neq 0$.

(б) *Для любой точки v поля k образ t_v элемента t в группе $H^1(k_v, G)$ тривиален.*

Согласно лемме 8, существует конечный $G(\bar{k}/k)$-модуль B и элемент $x \in H^2(k, B)$, такой, что $x \neq 0$ и все его локальные образы x_v нулевые. Пусть S — полупростая группа, удовлетворяющая условиям леммы 9 относительно пары (B, x). Эти условия показывают, что центр Z группы S содержит B и что существует элемент $y \in H^1(k, Z/B)$, для которого $dy = x$. Обозначим через G группу S/B, и пусть t — образ y в группе $H^1(k, G)$. Покажем, что пара (G, t) удовлетворяет условиям теоремы:

(а) Пусть Δ: $H^1(k, G) \to H^2(k, B)$ — оператор взятия кограницы, определяемый точной последовательностью

$$0 \to B \to S \to G \to 0.$$

Коммутативная диаграмма

$$\begin{array}{ccc} H^1(k,\ Z/B) & \xrightarrow{d} & H^2(k,\ B) \\ \downarrow & & \downarrow \text{id} \\ H^1(k,\ G) & \xrightarrow{\Delta} & H^2(k,\ B) \end{array}$$

показывает, что $\Delta(t) = dy = x$. Поскольку $x \neq 0$, получаем, что $t \neq 0$.

(б) Воспользуемся точной последовательностью

$$H^1(k_v,\ S) \to H^1(k_v,\ G) \to H^2(k_v,\ B).$$

Вышеприведенное рассуждение показывает, что $\Delta(t_v) = x_v = 0$, так как $H^1(k_v,\ S) = 0$ (ср. лемма 9), получаем $t_v = 0$, что и требовалось доказать.

Замечания. 1. Предыдущая конструкция неизбежно приводит к группам, которые лежат „строго между" односвязными и присоединенными группами. В этих двух крайних случаях „принцип Хассе", возможно, верен [1]). В случае односвязных групп можно даже сформулировать следующую гипотезу:

Каноническое отображение $H^1(k,\ G) \to \prod H^1(k_v,\ G)$ биективно (произведение берется по точкам v, для которых $k_v = \mathbf{R}$).

Эта гипотеза проверена для некоторых классических групп, а также для групп $\mathbf{G}_2$ и $\mathbf{F}_n$.

2. Т. Оно для получения полупростой группы, *число Тамагавы которой не является целым числом*, воспользовался построением, близким к конструкции леммы 9. Это наводит на следующий вопрос, поставленный Борелем: есть ли связь между числом Тамагавы и справедливостью принципа Хассе [2])?

БИБЛИОГРАФИЧЕСКИЕ УКАЗАНИЯ К ГЛАВЕ III

Содержание § 1 „хорошо известно", однако нигде не изложено удовлетворительно, не исключая и настоящего курса. Гипотезы 1 и 2 были высказаны на коллоквиуме

---

[1]) „Принцип Хассе" в односвязном случае был доказан Г. Хардером для групп, не содержащих множителей типа $\mathbf{E}_8$.

[2]) Вопрос, поставленный Борелем, решен Оно [3].

в Брюсселе в 1962. Теоремы 1, 2, 3 принадлежат Спрингеру; первые две можно найти в его докладе в Брюсселе, теорему 3 он мне сообщил непосредственно. Как показал Гротендик (не опубликовано), можно доказать несколько более сильный результат, воспользовавшись обращением в нуль „неабелевой H^2“ для любого поля, размерность которого не превосходит 1.

Параграф 4 почти без изменения извлечен из статьи Бореля, Серра [1]; я лишь добавил конструкцию контрпримера к принципу Хассе.

* * *

Наконец, вот краткий перечень работ, посвященных различным типам полупростых групп и содержащих (явно или нет) результаты о когомологиях Галуа:

Ортогональная группа: Э. Витт [1], Т. Спрингер [1].

Классические группы и алгебры с инволюцией: А. Вейль [3].

Группа $\mathbf{G}_2$: Джекобсон [1].

Группа $\mathbf{F}_4$: Альберт, Джекобсон [1].

Группа $\mathbf{E}_6$: Т. Спрингер [3].

ПРИЛОЖЕНИЕ

ДВОЙСТВЕННОСТЬ ДЛЯ КОГОМОЛОГИЙ ПРОКОНЕЧНЫХ ГРУПП

Жан-Луи Вердье

§ 1. ИНДУЦИРОВАННЫЕ И КОИНДУЦИРОВАННЫЕ МОДУЛИ

1.1. Определения. Пусть G — проконечная группа, V – ее открытая подгруппа и Y — дискретный топологический V-модуль. В п. 5 § 2 гл. I был определен индуцированный модуль $M_G^V(Y)$. Определим *коиндуцированный* модуль ${}_G^VM(Y)$, полагая

$${}_G^VM(Y) = \mathbf{Z}(G) \underset{\mathbf{Z}(V)}{\otimes} Y.$$

На нем можно определить структуру G-модуля, используя действие G на первом сомножителе. Проверяется, что это дискретный топологический G-модуль (согласно терминологии [GL], это индуцированный модуль).

Пусть X — дискретный топологический G-модуль. Обозначим через X^0 его же, но рассматриваемый как V-модуль, и положим $X_V = {}_G^VM(X^0)$ и ${}_VX = M_G^V(X^0)$. Тогда X_V — контравариантный функтор от X и ковариантный функтор от V. Действительно, для всякой открытой подгруппы $V' \subset G$, содержащейся в V, очевидным образом определяется отображение $X_{V'} \to X_V$. Аналогично ${}_VX$ — ковариантный функтор от X и контравариантный от V.

Изучим функторы X_V и ${}_VX$.

1.2. Предложение. *Бифунктор $(V, X) \to X_V$ канонически изоморфен бифунктору $(V, X) \to \mathbf{Z}(G/V) \otimes_{\mathbf{Z}} X$. Группа G действует на последнем модуле следующим образом:*

$$g\colon\ z \otimes x \to yz \otimes yx,\ \ g \in G,\ \ x \in X,\ \ z \in \mathbf{Z}(G/V).$$

Аналогично, бифунктор ${}_VX$ изоморфен бифунктору

$$(V, X) \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}(G/V), X),$$

на котором группа G действует следующим образом:

$$(ga)(z) = g(a(g^{-1}(z))),\ a \in \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}(G/V), X),$$
$$z \in \mathbf{Z}(G/V),\ g \in G.$$

Укажем только, как определяются изоморфизмы. Обозначим через g^0 класс элемента $g \in G$ в факторгруппе G/V. Поставим в соответствие каждому элементу $g \otimes x \in X_V$ элемент $g^0 \otimes gx$, принадлежащий модулю $\mathbf{Z}(G/V) \otimes_{\mathbf{Z}} X$. Проверяется, что таким образом получается изоморфизм X_V на $\mathbf{Z}(G/V) \otimes_{\mathbf{Z}} X$, функториальный относительно X и V. Аналогично, каждому элементу $a \in {}_V X$, т. е. каждому непрерывному отображению a: $G \to X$, удовлетворяющему условию

$$a(vg) = va(g), \quad v \in V, \quad g \in G,$$

соответствует отображение $\hat{a}$: $G \to X$: $g \to ga(g^{-1})$. Проверяется, что отображение $\hat{a}$ пропускается через G/V, а следовательно, определяет элемент из $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}(G/V), X)$. Далее легко проверяется, что так определенное отображение есть изоморфизм, функториальный по X и V.

Обозначим для краткости через X_V и ${}_V X$ функторы $\mathbf{Z}(G/N) \otimes_{\mathbf{Z}} X$ и $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}(G/V), X)$ соответственно. Свойства этих функторов устанавливаются в следующем предложении:

1.3. Предложение. 1) *Существуют трифункториальные изоморфизмы*

$$\mathrm{Hom}_G(X_V, Y) \xrightarrow{\sim} \mathrm{Hom}_G(X, {}_V Y) \xrightarrow{\sim} \mathrm{Hom}_V(X, Y).$$

2) *Для данной открытой подгруппы V существует некоторый функториальный по X изоморфизм i_V: $X_V \to {}_V X$. Очевидно, относительно V этот изоморфизм не может быть функториальным.*

3) *Функторы $X \to X_V$ и $X \to {}_V X$ точны по X и коммутируют с произвольными индуктивными и проективными пределами.*

4) *Если X — инъективный G-модуль, то G-модули X_V и ${}_V X$ также инъективны.*

5) *Пусть V' — открытая подгруппа G, содержащая и нормализующая V. С помощью вложения V'/V в G/V группа V' действует справа на $X_V \xrightarrow{\sim} \mathbf{Z}(G/V) \otimes_{\mathbf{Z}} X$.*

Эта структура правого V'-модуля функториальна по X в следующем смысле: Пусть U — открытая подгруппа в G, содержащаяся в V и инвариантная в V'. Каноническое отображение $X_U \to X_V$ согласовано со структурой V'-модуля.

Кроме того, группа V' действует слева на ${}_VX = \operatorname{Hom}_{\mathbf{Z}}(\mathbf{Z}(G/V), X)$ с помощью вложения V'/V в G/V. Действия V' перестановочны с действиями группы G. Эта структура левого V'-модуля функториальна по X и V.

Если отобразить правый V'-модуль X_V в левый V'-модуль ${}_VX$, положив

$$v' * x = x v'^{-1},$$

то изоморфизм i_V из (2) является изоморфизмом V'-модулей.

6) *Рассматривая X_V как правый V'/V-модуль, получаем, что*

$$H^i(V'/V, X_V) = 0 \quad \text{для} \quad i \neq 0 \quad \text{и} \quad H^0(V'/V, X_V) = X_{V'}.$$

6′) *Рассматривая ${}_VX$ как левый V'/V-модуль, получаем, что*

$$H^i(V'/V, {}_VX) = 0 \quad \text{для} \quad i \neq 0 \quad \text{и} \quad H^0(V'/V, {}_VX) = {}_{V'}X.$$

Доказательство. Если пользоваться вторым определением функторов X_V и ${}_VX$, то первое утверждение становится тривиальным. Изоморфизм i_V из второго утверждения получается при рассмотрении канонического базиса $\mathbf{Z}(G/V)$. Свойства (3) и (4) формально следуют тогда из свойств (1) и (2). Доказательство свойства (5) сводится к нескольким тривиальным проверкам. Докажем свойства (6) и (6′). Модуль $\mathbf{Z}(G/V)$ есть индуцированный правый V'/V-модуль. Отсюда следует, что X_V и ${}_VX$ — также индуцированные V'/V-модули. Остается показать, что $H^0(V'/V, X_V) = X_{V'}$ и что $H^0(V'/V, {}_VX) = {}_{V'}X$, но это очевидно.

Мы воспользуемся индуцированными модулями для построения резольвент.

Более точно, пусть X — дискретный G-модуль, X^0 — он же, рассматриваемый как абелева группа, $K^0(X) = M_G(X^0)$ — соответствующий индуцированный модуль, $\varepsilon(X)\colon X \to K^0(X)$ — каноническая инъекция. Положим

$Z^1(X) = \operatorname{Coker}(\varepsilon(X))$ и обозначим через $j^1(X)$: $K^0(X) \to Z^1(X)$ канонический морфизм. Определим по индукции для любого целого $i \geqslant 1$

$$K^i(X) = K^0(Z^i(X)), \quad \varepsilon^i = \varepsilon(Z^i(X)),$$
$$Z^{i+1}(X) = \operatorname{Coker}(\varepsilon^i), \quad j^{i+1} = j^1(Z^i(X)),$$
$$d^{i-1} = \varepsilon^i \circ j^i.$$

Тем самым получаем комплекс $K^*(X)$, функториальный по X, и функториальный морфизм

$$\varepsilon\colon \quad \mathrm{id} \to K^*,$$

превращающий комплекс $K^*(X)$ в резольвенту X.

1.4. Предложение. *K^* — аддитивный точный ковариантный функтор, коммутирующий с фильтрующимися индуктивными пределами, а G-модуль $K^i(X)$ когомологически тривиален (т. е.* $\operatorname{cd}(G, K^j(X)) = 0$, ср. гл. I, дополнение, стр. 85) *для любого положительного числа i и любого дискретного G-модуля X.*

Последнее условие очевидно, так как $K^i(X)$ — индуцированные модули. Для доказательства первого утверждения достаточно проверить, что $K^0(X)$ — точный функтор по X и что он коммутирует с фильтрующимися индуктивными пределами. Пусть

$$0 \to X' \to X \to X'' \to 0$$

— точная последовательность дискретных G-модулей. Соответствующая последовательность абелевых групп

$$0 \to X'^0 \to X^0 \to X''^0 \to 0$$

также точна.

Отсюда немедленно следует, что последовательность

$$0 \to M_G(X'^0) \to M_G(X^0) \to M_G(X''^0) \to 0$$

точна. Пусть теперь X_α — фильтрующаяся индуктивная система дискретных G-модулей и $X = \varinjlim_\alpha X_\alpha$. Пусть m — канонический морфизм

$$\varinjlim_\alpha (K^0(X_\alpha)) \to K^0(X),$$

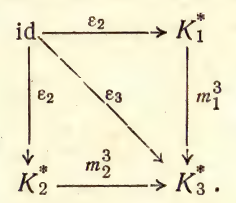
Этот морфизм, очевидно, инъективен; докажем, что он сюръективен. Для этого достаточно показать, что каждое непрерывное отображение a: $G \to X$ пропускается через X_α. Но группа G компактна, а X дискретна; отсюда следует, что образ G при отображении a конечен. Следовательно, этот образ содержится в образе X_α в X.

1.5. Определение. Каждая резольвента X, обладающая свойствами из предложения 1.4 и функториальная по X, называется *резольвентным функтором* (ср. Гротендик [1], 2.25).

1.6. Предложение. *Пусть* (K_1^*, ε_1) *и* (K_2^*, ε_2) — *два резольвентных функтора. Существует резольвентный функтор* (K_3^*, ε_3) *и морфизмы резольвентных функторов*

$$m_1^3\colon K_1^* \to K_3^*, \qquad m_2^3\colon K_2^* \to K_3^*,$$

такие, что следующая диаграмма коммутативна



Пусть $K_3^*(X)$ — простой комплекс, ассоциированный с двойным комплексом $K_1^i(K_2^j(X))$. Так как функтор K_1^* точен, комплекс $K_3^*(X)$ ацикличен всюду, кроме размерности нуль. Функтор $X \to K_3^*(X)$ точен и коммутирует с индуктивными пределами. Кроме того, $K_3^i(X)$, будучи для всех $i \geqslant 0$ прямой суммой когомологически тривиальных G-модулей, когомологически тривиален. Наконец, морфизмы вложения комплексов $K_1^*(X)$ и $K_2^*(X)$ в двойной комплекс $K_1^i(K_2^j(X))$ определяют морфизмы

$$m_1^3\colon \quad K_1^* \to K_3^*,$$
$$m_2^3\colon \quad K_2^* \to K_3^*,$$

функториальные по X и индуцирующие изоморфизмы на когомологиях. Кроме того, коммутативна следующая диа-

грамма

$$\begin{array}{ccc} X & \xrightarrow{\varepsilon_1} & K_1^*(X) \\ \downarrow{\scriptstyle \varepsilon_2} & & \downarrow{\scriptstyle m_1^3} \\ K_2^*(X) & \xrightarrow{m_2^3} & K_3^*(X), \end{array}$$

позволяющая определить морфизм ε_3, что и завершает доказательство.

§ 2. ЛОКАЛЬНЫЕ ГОМОМОРФИЗМЫ

2.1. Определение. Пусть S — замкнутая подгруппа группы G, а X и Y — два дискретных G-модуля. Положим

$$\mathrm{Hom}_S(X, Y) = \\ = \varinjlim_{V \supset S} \mathrm{Hom}_V(X, Y) \xrightarrow{\sim} \varinjlim_{V \supset S} \mathrm{Hom}_G(X_V, Y) \xrightarrow{\sim} \varinjlim_{V \supset S} \mathrm{Hom}_G(X_V, Y),$$

где индуктивные пределы берутся по проективной системе открытых подгрупп V, содержащих S.

Назовем группу $\mathrm{Hom}_S(X, Y)$ *группой локальных гомоморфизмов относительно подгруппы* S. В случае когда $S = \{1\}$, обозначим $\mathrm{Hom}_S(X, Y)$ через $\mathrm{Hom}(X, Y)$.

2.2. Предложение. *Пусть U — замкнутая подгруппа группы G, содержащая и нормализующая S.*

1) *Группа U/S действует на* $\mathrm{Hom}_S(X, Y)$, *определяя на ней структуру дискретного топологического U/S-модуля; кроме того,*

$$H^0(U/S, \mathrm{Hom}_S(X, Y)) = \mathrm{Hom}_V(X, Y).$$

2) *Если модуль Y инъективен, то*

$$\mathrm{cd}_{U/S}(\mathrm{Hom}_S(X, Y)) = 0.$$

3) *Правыми производными функторами функтора $Y \to \mathrm{Hom}_S(X, Y)$ (со значениями в категории U/S-модулей) являются функторы*

$$\mathrm{Ext}_S^i(X, Y) = \\ = \varinjlim_{V \supset S} \mathrm{Ext}_V^i(X, Y) \xrightarrow{\sim} \varinjlim_{V \supset S} \mathrm{Ext}_G^i(X_V, Y) \xrightarrow{\sim} \varinjlim_{V \supset S} \mathrm{Ext}_G^i(X, {}_VY).$$

Доказательство. 1) Легко проверяется, что $\mathrm{Hom}_S(X, Y)$ — это наибольший подмодуль $\mathrm{Hom}_{\mathbf{Z}}(X, Y)$, на котором непрерывно действует группа G и для которого

$$\mathrm{Hom}(X, Y)^S = \mathrm{Hom}_S(X, Y).$$

Утверждение отсюда следует немедленно.

2) Надо показать, что для любой подгруппы U и любого целого числа $i \geqslant 0$

$$H^i(U/S, \mathrm{Hom}_S(X, Y)) = 0.$$

Но каждая открытая подгруппа V', содержащая S, содержит открытую подгруппу V, содержащую S и нормализуемую подгруппой U. Отсюда следует, что

$$H^0(U/S, \mathrm{Hom}_S(X, Y)) = \varinjlim_{V \supset S} H^0(U \cdot V/V, \mathrm{Hom}_V(X, Y)),$$

где предел берется по подгруппам V, нормализующим U. Таким образом, согласно гл. I, § 1, предл. 8, можно считать, что S открыта.

Пусть $Z^\cdot$ — резольвента (занумерованная целыми отрицательными числами) U/S-модуля $\mathbf{Z}$, состоящая из свободных U/S-модулей конечного типа. Тогда

$$H^*(U/S, \mathrm{Hom}_S(X, Y)) = H^*(\mathrm{Hom}^{\cdot}_{U/S}(Z^\cdot, \mathrm{Hom}_S(X, Y)))\ ^{1)}.$$

Но так как S открыта, $\mathrm{Hom}_S(X, Y) = \mathrm{Hom}_S(X, Y)$. Воспользовавшись каноническими изоморфизмами, получаем, что

$$H^*(U/S, \mathrm{Hom}_S(X, Y)) = H^*(\mathrm{Hom}^{\cdot}_U(X, \mathrm{Hom}^{\cdot}_{\mathbf{Z}}(Z^\cdot, Y))).$$

Члены комплекса $Z^\cdot$ суть прямые суммы модулей, изоморфных $\mathbf{Z}(U/S)$. Отсюда следует, что комплекс $\mathrm{Hom}^{\cdot}_{\mathbf{Z}}(Z^\cdot, Y)$ состоит из членов, являющихся прямыми суммами модулей, изоморфных $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}(U/S), Y)$. Но модуль Y является G-инъективным, а следовательно, U-инъективным. В силу предложения 1.3 получаем, что U-модуль $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}(U/S), Y)$ инъективен. Таким образом, комплекс $\mathrm{Hom}^{\cdot}_{\mathbf{Z}}(Z^\cdot, Y)$ состоит из инъективных U-модулей. Кроме того, модули когомологий этого комплекса все нулевые, за исключением размерности нуль, в которой $H^0(\mathrm{Hom}^{\cdot}_{\mathbf{Z}}(Z^\cdot, Y)) = Y$. Сле-

[1]) Где $\mathrm{Hom}^{\cdot}_{U/S}$ обозначает комплекс морфизмов.

довательно, комплекс $\mathrm{Hom}_{\dot{Z}}(Z^{\cdot}, Y)$ есть инъективная резольвента U-модуля Y. Таким образом

$$H^{*}(U/S, \mathbf{Hom}_S(X, Y)) = \mathrm{Ext}_U^{*}(X, Y).$$

Но модуль Y G-инъективен, а потому и U-инъективен, что и требовалось доказать.

3) Утверждение очевидно.

2.3. Следствие. *Существует спектральная последовательность*

$$E_2^{p,q} = H^p(U/S, \mathbf{Ext}_S^q(X, Y)) \Rightarrow \mathbf{Ext}_U^{p+q}(X, Y).$$

Эта спектральная последовательность композиции функторов, применимая здесь в силу предложения 2.2 (2) [1].

2.4. Предложение. *В случае когда модуль X конечного типа (как абелева группа или как G-модуль, что одно и то же) или когда подгруппа S открыта,*

$$\mathbf{Hom}_S(X, Y) = \mathrm{Hom}_S(X, Y),$$
$$\mathbf{Ext}_S^i(X, Y) = \mathrm{Ext}_S^i(X, Y).$$

Случай, когда S открыта, тривиален. Предположим что X конечного типа. Группа G действует в этом случае на X посредством G/V', где V' — достаточно малый открытый нормальный делитель. Отсюда следует, что для любой достаточно малой открытой подгруппы V

$$\mathbf{Hom}_V(X, Y) = \mathrm{Hom}_Z(X, Y^V),$$

а, следовательно, поскольку X как абелева группа конечного типа,

$$\mathbf{Hom}(X, Y) = \mathrm{Hom}_Z(X, Y).$$

Отсюда легко следует предложение.

2.5. Следствие. *Если подгруппа U открыта (например, $U = G$), то спектральная последовательность* 2.3 *принимает вид*

$$H^p(U/S, \mathbf{Ext}_S^q(X, Y)) \Rightarrow \mathrm{Ext}_U^{p+q}(X, Y).$$

Если к тому же модуль X конечного типа или подгруппа S открыта, то спектральную последовательность

---

[1] См. Гротендик [1], теорема 2.4.1.

можно записать в виде

$$H^p\big(U/S,\ \mathrm{Ext}^q_S(X,\ Y)\big) \Rightarrow \mathrm{Ext}^{p+q}_U(X,\ Y).$$

В частности, когда X — модуль конечного типа,

$$H^p\big(U,\ \mathrm{Ext}^q_{\mathbf{Z}}(X,\ Y)\big) \Rightarrow \mathrm{Ext}^{p+q}_U(X,\ Y).$$

Эта спектральная последовательность дает бесконечную точную последовательность

$$0 \to H^1(U,\ \mathrm{Hom}_{\mathbf{Z}}(X,\ Y)) \to \mathrm{Ext}^1_U(X,\ Y) \to$$
$$\to H^0\big(U,\ \mathrm{Ext}^1_{\mathbf{Z}}(X,\ Y)\big) \xrightarrow{\delta} H^2(U,\ \mathrm{Hom}_{\mathbf{Z}}(X,\ Y)) \to \ldots$$
$$\ldots \to H^p(U,\ \mathrm{Hom}_{\mathbf{Z}}(X,\ Y)) \to \mathrm{Ext}^p_U(X,\ Y) \to$$
$$\to H^{p-1}\big(U,\ \mathrm{Ext}^1_{\mathbf{Z}}(X,\ Y)\big) \xrightarrow{\delta} H^{p+1}(U,\ \mathrm{Hom}_{\mathbf{Z}}(X,\ Y)) \to \ldots$$

2.6. Замечания. 1. Пусть V — открытый нормальный делитель группы G. Для любой пары G-модулей X и Y абелеву группу $\mathrm{Ext}^i_V(X,\ Y)$ можно снабдить структурой G/V-модуля. Эта структура определяется следующим образом: $\mathrm{Ext}^i_V(X,\ Y)$ функториально изоморфна $\mathrm{Ext}^i_G(X_V,\ Y)$, с другой стороны, группа X_V снабжена структурой правого G/V-модуля, а следовательно, для любого контравариантного функтора F со значениями в категории абелевых групп $F(X_V)$ является левым G/V-модулем.

Пусть S — замкнутый нормальный делитель группы G. Предыдущее замечание легко позволяет определить на $\mathrm{Ext}^i_S(X,\ Y)$ структуру G/S-модуля. Действительно, G/S-модуль $\mathrm{Ext}^i_S(X,\ Y)$ есть индуктивный предел G/S-модулей $\mathrm{Ext}^i_V(X,\ Y)$, где предел берется по открытым нормальным делителям V, содержащим S.

2. Если $X = \mathbf{Z}$, то $\mathrm{Ext}^i_V(\mathbf{Z},\ Y) = H^i(V,\ Y)$ снабжается таким образом структурой G/V-модуля. Предположим, что группа G тривиально действует на Y. Структура G/V-модуля на $H^i(V,\ Y)$ получается в этом случае с помощью действия G на V внутренними автоморфизмами.

3. Пусть V — открытая подгруппа в G, а X — некоторый G-модуль. В этом случае определены изоморфизмы

$$H^i(V,\ X) \xrightarrow{\sim} H^i(G,\ {}_VX) \xrightarrow{\sim} H^i(G,\ X_V),$$

первый изоморфизм определен, исходя из изоморфизмов предложения 1.3 (1), а второй — с помощью изоморфизма i_V: $X_V \to {}_VX$, определенного в предложении 1.3 (2). Пусть V' — открытый нормальный делитель группы G, содержащий V. Канонический гомоморфизм ${}_VX \to {}_{V'}X$ определяет тогда канонический гомоморфизм $H^i(Y, X) \to H^i(V', X)$, который совпадает просто с отображением *ограничения*. Аналогично, канонический гомоморфизм $X_{V'} \to X_V$ определяет гомоморфизм $H^i(V', X) \to H^i(V, X)$, совпадающий с *коограничением*.

§ 3. ТЕОРЕМА ДВОЙСТВЕННОСТИ

Обозначим через $\mathscr{C}$ одну из следующих категорий:

$\mathscr{C}_G$ — категория дискретных топологических G-модулей.

$\mathscr{C}_G^t$ — полная подкатегория категории $\mathscr{C}_G$, состоящая из периодических G-модулей.

$\mathscr{C}_G^p$ — полная подкатегория $\mathscr{C}_G$, состоящая из p-периодических G-модулей.

Для сокращения записи обозначим функтор $H^0(G, \cdot)$ через Γ. Пусть $X^{\cdot}$ и $Y^{\cdot}$ — два комплекса произвольной аддитивной категории; обозначим через $\mathrm{Hom}^{\cdot}(X^{\cdot}, Y^{\cdot})$ простой комплекс морфизмов $X^{\cdot}$ в $Y^{\cdot}$.

Если идет речь о резольвентном функторе (определение 1.5), то считается, что он принимает значение в категории $\mathscr{C}$, а не только в $\mathscr{C}_G$. Функтор K^* из предложения 1.4 на объектах из категории $\mathscr{C}$ принимает значения в категории $\mathscr{C}$.

3.1. Предложение. *Пусть A — абелева группа, $X \to K^*(X)$ — резольвентный функтор.*

1) *Функтор*

$$X \to \mathrm{Hom}^{\cdot}_{\mathrm{Ab}}(\Gamma K^*(X), A)$$

на категории $\mathscr{C}$, принимающий значения в категории комплексов абелевых групп, представим. Другими словами, существует комплекс $\tilde{\Gamma}_{\mathscr{C}}(A)$ объектов категории $\mathscr{C}$ и функторный изоморфизм

$$\Delta\colon \mathrm{Hom}^{\cdot}_{\mathrm{Ab}}(\Gamma K^*(X), A) \xrightarrow{\sim} \mathrm{Hom}^{\cdot}_{\mathscr{C}}(X, \tilde{\Gamma}_{\mathscr{C}}(A)).$$

Комплекс $\tilde{\Gamma}_{\mathscr{C}}(A)$ *функториален по* A. *Функтор* $A \to \tilde{\Gamma}_{\mathscr{C}}(A)$ *определен однозначно, с точностью до изоморфизма.*

2) *Комплекс* $\tilde{\Gamma}_{\mathscr{C}}(A)$ *не зависит, с точностью до гомотопии, от выбора резольвентного функтора.*

3) *Если* A — *инъективная абелева группа, то объекты комплекса* $\tilde{\Gamma}_{\mathscr{C}}(A)$ *инъективны.*

4) *Пусть* $X \to K^*(X)$ — *резольвентный функтор на категории* $\mathscr{C}_G$, *принимающий значения на объектах* X *из категории* $\mathscr{C}_G^t$ (*соответственно* $\mathscr{C}_G^p$) *в категории* $\mathscr{C}_G^t$ (*соответственно* $\mathscr{C}_G^p$). *Тогда* $\tilde{\Gamma}_{\mathscr{C}_G^t}(A)$ — *периодический подкомплекс комплекса* $\tilde{\Gamma}_{\mathscr{C}_G}(A)$, *а комплекс* $\tilde{\Gamma}_{\mathscr{C}_G^p}(A)$ — p-*примарная часть* $\tilde{\Gamma}_{\mathscr{C}_G^t}(A)$.

5) *Если* A — *инъективная абелева группа, то объекты когомологий комплекса* $\tilde{\Gamma}_{\mathscr{C}}(A)$ *даются следующими формулами:*

а) $\mathscr{C} = \mathscr{C}_G$,

$$H^{-q}\left(\tilde{\Gamma}_{\mathscr{C}_G}(A)\right) = \varinjlim_{V,\,\mathrm{Cor}} \mathrm{Hom}_{\mathbf{Z}}(H^q(V,\,\mathbf{Z}),\,A),$$

где индуктивный предел берется по открытым подгруппам и морфизмам коограничения. Структура G-*модуля определяется структурой правого* G-*модуля* $H^q(V,\,\mathbf{Z})$, *где* V — *нормальный делитель в* G.

б) $\mathscr{C} = \mathscr{C}_G^t$,

$$H^{-q}\left(\tilde{\Gamma}_{\mathscr{C}_G^t}(A)\right) = \varinjlim_{V,\,\mathrm{Cor},\,m} \mathrm{Hom}_{\mathbf{Z}}(H^q(V,\,\mathbf{Z}/m\mathbf{Z}),\,A).$$

в) $\mathscr{C} = \mathscr{C}_G^p$,

$$H^{-q}\left(\tilde{\Gamma}_{\mathscr{C}_G^p}(A)\right) = \varinjlim_{V,\,\mathrm{Cor},\,m} \mathrm{Hom}_{\mathbf{Z}}(H^q(V,\,\mathbf{Z}/p^m\mathbf{Z}),\,A).$$

Доказательство. 1) Свойства резольвентных функторов (определение 5) показывают, что функтор

$$X \to \mathrm{Hom}\,(\Gamma K^i(X),\,A)$$

контравариантен, точен слева и преобразует фильтрующиеся индуктивные пределы в фильтрующиеся проективные пределы. Так как категория $\mathscr{C}$ локально нётерова (см. диссертацию Габриэля [1], гл. 2), этот функтор представим (ср. диссертацию Габриэля, гл. 2, п. 4, или гл. 1, § 3, лемма 6). Отсюда легко следует утверждение.

2) Пусть K_1^* и K_2^* — два резольвентных функтора; для доказательства утверждения можно считать в силу предложения 1.6, что существует морфизм резольвент m: $K_1^* \to K_2^*$. Отсюда следует существование функториального по A изоморфизма $\tilde{m}$: $\tilde{\Gamma}_{\mathscr{C},1}(A) \to \tilde{\Gamma}_{\mathscr{C},2}(A)$, такого, что для любого объекта X категории $\mathscr{C}$ морфизм

$$\mathrm{Hom}^{\cdot}_{\mathscr{C}}(X, \tilde{\Gamma}_{\mathscr{C},1}(A)) \to \mathrm{Hom}^{\cdot}_{\mathscr{C}}(X, \tilde{\Gamma}_{\mathscr{C},2}(A)),$$

полученный из морфизма m, индуцирует изоморфизм на группах когомологий. Это показывает, что морфизм m, с точностью до гомотопии, является изоморфизмом.

3) Ясно.

4) Ясно.

5) Рассмотрим случай $\mathscr{C} = \mathscr{C}_G$. Изоморфизм Δ индуцирует на группах когомологий изоморфизм

$$\Delta_{-q}: \mathrm{Hom}_{\mathbf{Z}}(H^q(G, X), A) \to H^{-q}(\mathrm{Hom}_G(X, \tilde{\Gamma}_{\mathscr{C}_G}(A))).$$

Полагая $X = \mathbf{Z}_V$ и переходя к индуктивному пределу по открытым подгруппам, получаем нужный нам результат. Аналогично поступаем в других случаях.

Обозначим через $R(\mathrm{Ab})$ (соответственно $R(\mathscr{C})$) категорию конечных комплексов (т. е. комплексов, члены которых, за исключением конечного числа, все равны нулю) абелевых групп (соответственно объектов категории $\mathscr{C}$)[1]. Если функтор Γ имеет конечную когомологическую размерность на категории $\mathscr{C}$, то существуют конечные резольвентные функторы (т. е. такие, что для всех объектов X из $\mathscr{C}$ комплекс $K^*(X)$ конечен). Для резольвентного функтора, введенного в предложении 1.4, и достаточно

---

[1]) Морфизмы в категории $R(\mathrm{Ab})$ (соответственно $R(\mathscr{C})$) суть гомоморфизмы комплексов, сохраняющие степень и коммутирующие с дифференциалами.

больших i модули Z^i когомологически тривиальны. Итак, пусть $X \to K^*(X)$ — конечный резольвентный функтор. Продолжим его на категорию $R(\mathscr{C})$ следующим образом: пусть $X^{\cdot}$ — объект категории $R(\mathscr{C})$, тогда пусть

$K^*(X^{\cdot})$ — простой комплекс, ассоциированный с двойным комплексом $K^i(X^j)$.

3.2. Предложение. *Предположим, что функтор* Γ *имеет конечную когомологическую размерность на категории* $\mathscr{C}$. *Пусть* $X \to K^*(X)$ — *конечный резольвентный функтор,* $X^{\cdot}$ — *объект из* $R(\mathscr{C})$, $A^{\cdot}$ — *объект из* $R(\mathrm{Ab})$.

1) *Существует функтор* $A^{\cdot} \to \tilde{\Gamma}_{\mathscr{C}}(A^{\cdot})$, *принимающий значения в категории* $R(\mathscr{C})$, *и бифункториальный изоморфизм*

$$\Delta\colon \mathrm{Hom}^{\cdot}_{\mathrm{Ab}}(\Gamma K^*(X^{\cdot}),\ A^{\cdot}) \xrightarrow{\sim} \mathrm{Hom}^{\cdot}_{\mathscr{C}}\left(X^{\cdot},\ \tilde{\Gamma}_{\mathscr{C}}(A^{\cdot})\right).$$

2) *Изоморфизм* Δ *определяет гомоморфизм комплексов* (*т. е. гомоморфизм, коммутирующий с дифференциалами*) *нулевой степени* $\rho\colon \Gamma K^*\tilde{\Gamma}_{\mathscr{C}}(A^{\cdot}) \to A^{\cdot}$, *такой, что изоморфизм* Δ^{-1} *совпадает с композицией гомоморфизмов*

$$\mathrm{Hom}^{\cdot}_{\mathscr{C}}\left(X^{\cdot},\ \Gamma_{\mathscr{C}}(A^{\cdot})\right) \xrightarrow{\Gamma K^*} \mathrm{Hom}^{\cdot}_{\mathrm{Ab}}\left(\Gamma K^*(X^{\cdot}),\ \Gamma K^*\Gamma_{\mathscr{C}}(A^{\cdot})\right) \xrightarrow{\circ\rho} \to \mathrm{Hom}^{\cdot}_{\mathrm{Ab}}(\Gamma K^*(X^{\cdot}),\ A).$$

Доказательство. Утверждение 1 тривиально следует из предложения 3.1 (1). Для доказательства утверждения 2 используются классические доказательства из теории сопряженных функторов.

Пусть $X^{\cdot}$ — объект $R(\mathscr{C})$. Обозначим через $\mathbf{H}^i(G,\ X^{\cdot})$ i-ю группу гиперкогомологий $\Gamma(X^{\cdot})$; пусть, кроме того, $Y^{\cdot}$ — другой объект категории $R(\mathscr{C})$; обозначим через $\mathrm{Ext}^i_G(X^{\cdot},\ Y^{\cdot})$ i-й гипер-Ext (ср. Картан — Эйленберг [1], гл. 18, п. 2). Это обозначение, в котором не участвует $\mathscr{C}$, законно, потому что справедлива

3.3. Лемма. *Инъективный объект* I *категории* $\mathscr{C}$ *инъективен в* $\mathscr{C}_G$.

Так как случай $\mathscr{C} = \mathscr{C}_G$ тривиален, предположим, что $\mathscr{C} = \mathscr{C}^t_G$. Пусть J — инъективный объект категории $\mathscr{C}_G$.

Ясно, что периодический подобъект J^t объекта J инъективен в $\mathscr{C}_G^t$ и что любой объект категории $\mathscr{C}_G^t$ можно погрузить в инъективный объект такого вида. Таким образом, достаточно показать, что J^t инъективен в $\mathscr{C}_G$. Но J, будучи инъективным объектом, является прямым слагаемым индуцированного инъективного модуля $M_G(J^0)$, где J^0 обозначает объект J, рассматриваемый как инъективная абелева группа. Отсюда получаем, что J — прямое слагаемое объекта $M_G(J^0)^t = M_G(J^{0t})$, который инъективен в $\mathscr{C}_G$.

Случай $\mathscr{C} = \mathscr{C}_G^p$ разбирается аналогично.

3.4. Определение. Дуализирующим комплексом категории $\mathscr{C}$ называется *конечный комплекс* $D^{\cdot}$ *категории* $\mathscr{C}$, *снабженный гомоморфизмом* ρ: $\mathbf{H}^0(G, D^{\cdot}) \to \mathbf{Q}/\mathbf{Z}$, таким, что композиция гомоморфизмов

$$\mathbf{H}^i(G, X^{\cdot}) \times \mathbf{Ext}_G^{-i}(X^{\cdot}, D^{\cdot}) \xrightarrow{\smile} \mathbf{H}^0(G, D^{\cdot}) \xrightarrow{\rho} \mathbf{Q}/\mathbf{Z}$$

(где первая стрелка определяется $\smile$-произведением) определяет функторные изоморфизмы $\mathbf{Ext}_G^{-i}(X^{\cdot}, D^{\cdot}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}}(\mathbf{H}^i(G, X^{\cdot}), \mathbf{Q}/\mathbf{Z})$. Однозначность (в некотором смысле) дуализирующего комплекса устанавливается предложением, которое следует ниже. Пусть $X^{\cdot}$ — объект из $R(\mathscr{C})$. Инъективная резольвента объекта $X^{\cdot}$ — это гомоморфизм $X^{\cdot}$ в комплекс $\mathrm{Inj}(X^{\cdot})$, все объекты которого принадлежат категории $\mathscr{C}$, инъективны в ней и, за исключением конечного числа, равны нулю в отрицательных степенях; этот гомоморфизм индуцирует изоморфизм когомологий. Инъективные резольвенты существуют (Картан, Эйленберг [1], гл. 17) и определяются однозначно с точностью до гомотопии.

3.5. Предложение. *Пусть* $(D_1^{\cdot}, \rho_1)$ *и* $(D_2^{\cdot}, \rho_2)$ — *два дуализирующих комплекса категории* $\mathscr{C}$, *а* $\mathrm{Inj}(D_1^{\cdot})$ *и* $\mathrm{Inj}(D_2^{\cdot})$ — *их инъективные резольвенты. Существует единственный, с точностью до гомотопии, гомоморфизм*

$$s\colon \mathrm{Inj}(D_1^{\cdot}) \to \mathrm{Inj}(D_2^{\cdot}),$$

согласованный с отображениями ρ_1 *и* ρ_2.

Доказательство этого предложения мы опускаем.

3.6. Теорема. *Пусть G — проконечная группа конечной когомологической размерности (соответственно конечной когомологической p-размерности). Категории $\mathscr{C}_G$, $\mathscr{C}_G^t$ (соответственно $\mathscr{C}_G^p$) обладают дуализирующими комплексами.*

Действительно, изоморфизм Δ из предложения 3.2 дает при переходе к когомологиям изоморфизмы

$$\Delta_{-q}\colon \mathrm{Hom}_{\mathbf{Z}}\big(\mathbf{H}^q(G, X^{\cdot}),\ \mathbf{Q}/\mathbf{Z}\big) \xrightarrow{\sim} \mathbf{Ext}_G^{-q}(X^{\cdot},\ \Gamma_{\mathscr{C}}(\mathbf{Q}/\mathbf{Z})).$$

Утверждение 2 из предложения 3.2 позволяет определить, кроме того, гомоморфизм

$$\rho\colon\ \mathbf{H}^0(G,\ \Gamma_{\mathscr{C}}(\mathbf{Q}/\mathbf{Z})) \to \mathbf{Q}/\mathbf{Z},$$

вторая же часть этого утверждения показывает, что из определения $\smile$-произведения следует, что изоморфизм Δ_{-q}^{-1} определяется композицией гомоморфизмов

$$\mathbf{Ext}_G^{-q}(X^{\cdot},\ \Gamma_{\mathscr{C}}(\mathbf{Q}/\mathbf{Z}))\times$$
$$\times\, \mathbf{H}^q(G,\ X^{\cdot}) \xrightarrow{\smile} \mathbf{H}^0(G,\ \Gamma_{\mathscr{C}}(\mathbf{Q}/\mathbf{Z})) \xrightarrow{\rho} \mathbf{Q}/\mathbf{Z}.$$

Обозначим через $\tilde{I}$ (соответственно $\tilde{I}^t$ или $\tilde{I}^p$) комплекс инъективных G-модулей $\tilde{\Gamma}_{\mathscr{C}_G}(\mathbf{Q}/\mathbf{Z})$ (соответственно $\tilde{\Gamma}_{\mathscr{C}_G^t}(\mathbf{Q}/\mathbf{Z})$ или $\tilde{\Gamma}_{\mathscr{C}_G^p}(\mathbf{Q}/\mathbf{Z})$), определяемый, согласно предложению 3.1, произвольным резольвентным функтором[1]). Объекты когомологий этого комплекса даются формулами из предложения 3.1 (5). Выбор другого резольвентного функтора приводит к замене комплексов $\tilde{I}$, $\tilde{I}^t$, $\tilde{I}^p$ на гомотопически эквивалентные им комплексы. Если, например, группа G имеет конечную когомологическую размерность, то комплекс $\tilde{I}$ гомотопен конечному инъективному комплексу и теорема 3.6 показывает, что изоморфизм ∂-функторов

$$\Delta_{-q}\colon \mathrm{Hom}_{\mathbf{Z}}\big(H^q(G,\ X),\ \mathbf{Q}/\mathbf{Z}\big) \to H^{-q}\big(\mathrm{Hom}_G^{\cdot}(X,\ \tilde{I})\big),$$
$$X \in \mathrm{ob}\,(\mathscr{C}_G)$$

[1]) Если это не ведет к путанице, мы будем просто писать I (соответственно I^t, I^p).

(введенный в предложении 3.1 без всяких ограничений на G) определяется $\smile$-произведением.

3.7. Предложение. *Пусть G — проконечная группа, а H — группа, действующая на G и обладающая следующим свойством: для любой открытой подгруппы V группы G существует открытая подгруппа V', содержащаяся в V и инвариантная относительно H и G.*

В этом случае группа H действует на $H^{-q}(\tilde{I})$ для любого целого числа q, и если обозначить через h_q действие, соответствующее элементу $h \in H$, то имеет место формула

$$h_q(g_\alpha) = h(g)\, h_q(\alpha), \quad g \in G, \quad \alpha \in H^{-q}(\tilde{I}).$$

Другими словами, группа H действует на G-модуле $H^{-q}(\tilde{I})$ согласованно с автоморфизмами H на G.

В частности, если $H = G$ и G действует на себе внутренними автоморфизмами, то действие группы G на $H^{-q}(\tilde{I})$ совпадает с естественным действием G на $H^{-q}(\tilde{I})$.

Кроме того, аналогичный результат справедлив для комплексов $\tilde{I}^t$ и $\tilde{I}^p$.

Действительно, согласно предложению 3.1,

$$H^{-q}(\tilde{I}) = \varinjlim_{V,\, \mathrm{Cor}} \mathrm{Hom}_{\mathbf{Z}}\left(H^q(V, \mathbf{Z}), \mathbf{Q}/\mathbf{Z}\right).$$

Если подгруппа V инвариантна относительно H и G, то действие H на $\mathrm{Hom}_{\mathbf{Z}}(H^q(V, \mathbf{Z}), \mathbf{Q}/\mathbf{Z})$ согласовано с действием G, получаемым из действия G на V внутренними автоморфизмами. Переходя к индуктивному пределу, приходим к нужному нам результату. Это же рассуждение применяется к комплексам $\tilde{I}^t$ и $\tilde{I}^p$.

3.8. Предложение. *Пусть G — проконечная группа, а V — ее открытый нормальный делитель.*

1) *V-модуль $H^{-q}(\tilde{I}_V)$ канонически изоморфен V-модулю, полученному из G-модуля $H^{-q}(\tilde{I}_G)$ операцией сужения скаляров.*

2) *Наоборот, когда G действует на V внутренними автоморфизмами, выполняется условие предложения 3.7*

и, следовательно, группа G действует на $H^{-q}(I_V)$. Получаемый таким образом G-модуль канонически изоморфен $H^{-q}(I_G)$.

Аналогичный результат справедлив для комплексов $\tilde{I}^t$ и $\tilde{I}^p$.

Доказательство. Первое утверждение, очевидно, следует из формул предложения 3.1. Второе немедленно получается из предложения 3.7.

Эти два последних предложения позволяют определить дуализирующий комплекс группы G по дуализирующему комплексу подгруппы V.

§ 4. ПРИЛОЖЕНИЕ ТЕОРЕМЫ ДВОЙСТВЕННОСТИ

4.1. Определение. Пусть G — проконечная группа и p — простое число. Группа G называется *группой Коэна — Маколея в строгом смысле относительно p*, если

1) G — группа конечной когомологической p-размерности;

2) комплекс $\tilde{I}^p_G$ имеет только один отличный от нуля объект когомологий;

3) объекты когомологий комплекса $\tilde{I}^p_G$ инъективны как абелевы группы.

4.2. Замечания. 1. Если G — группа Коэна — Маколея в строгом смысле относительно p и $\mathrm{cd}_p(G) = n$, то ненулевой объект когомологий комплекса $\tilde{I}^p_G$ есть $H^{-n}(\tilde{I}^p_G)$ и, следовательно, он совпадает с дуализирующим модулем группы G (ср. гл. 1, § 3, п. 5.2).

2. По аналогии с теорией двойственности для локальных колец[1]) мы называем G *группой Коэна — Маколея*

[1]) Автор имеет в виду теорию двойственности для локальных когомологий. Основной результат этой теории состоит в следующем: пусть A — полное локальное кольцо размерности n, $\mathfrak{m}$ — его максимальный идеал. Для любого A-модуля конечного типа M положим $H^i_{\{\mathfrak{m}\}}(M) = \varinjlim_n \mathrm{Ext}^i(A/\mathfrak{m}^n, M)$. Тогда если A — кольцо Коэна — Маколея (см. Серр [7*]), то имеет место

относительно p, если она обладает первыми двумя свойствами из определения 4.1. Пример группы Коэна — Маколея, не являющейся группой Коэна — Маколея в строгом смысле, мне неизвестен.

Пусть G — группа Коэна — Маколея относительно p. Обозначим через $\hat{I}^p = H^{-n}(\tilde{I}^p_G)$ ($n = \mathrm{cd}_p(G)$) дуализирующий модуль группы G. Теорему двойственности можно в этом случае записать в виде изоморфизма

$$\Delta_{-q}\colon \mathrm{Hom}_{\mathbf{Z}}(H^q(G, X), \mathbf{Q}/\mathbf{Z}) \xrightarrow{\sim} \mathrm{Ext}^{n-q}_G(X, \hat{I}^p), \; X \in \mathrm{Ob}(\mathscr{C}^p_G).$$

Действительно, за дуализирующий комплекс можно взять комплекс, сводящийся к единственному объекту $\hat{I}^p$ в размерности $-n$ и нулю в других размерностях. Изоморфизм двойственности определяется с помощью $\cup$-произведения и канонического гомоморфизма ρ: $H^n(G, I^p) \to \mathbf{Q}/\mathbf{Z}$.

Положим $H^q(G) = H^q(G, \mathbf{Z}/p\mathbf{Z})$.

4.3. Предложение. *Пусть G — такая проконечная группа, что $\mathrm{cd}_p(G) = n$. Следующие два условия эквивалентны*:

1) *G является группой Коэна — Маколея в строгом смысле относительно p*;

2) *Для всех $q \neq n$* $\varinjlim_{V,\,\mathrm{Cor}} \mathrm{Hom}_{\mathbf{Z}}(H^q(V), \mathbf{Q}/\mathbf{Z}) = \{0\}$.

Доказательство. 1) $\Rightarrow$ 2). Полагая в формуле двойственности $X = \mathbf{Z}/p\mathbf{Z}_V$, получаем изоморфизм

$$\mathrm{Hom}_{\mathbf{Z}}(H^q(V), \mathbf{Q}/\mathbf{Z}) \xrightarrow{\sim} \mathrm{Ext}^{n-q}_V(\mathbf{Z}/p\mathbf{Z}, \hat{I}^p).$$

Переходя к индуктивному пределу по открытым подгруппам, получаем искомый результат. (Надо использовать предложение 2.4.)

невырожденное спаривание

$$H^i_{\{\mathfrak{m}\}}(M) \times \mathrm{Ext}^{n-i}(M, \Omega) \to I,$$

где I — инъективная оболочка поля вычетов кольца A (ср. Габриэль [1]), а $\Omega = \mathrm{Hom}\left(H^n_{\{\mathfrak{m}\}}(A), I\right)$. В частности, если A — регулярное кольцо, то $I = H^n_{\{\mathfrak{m}\}}(A)$ и $\Omega = A$. Подробное изложение этой теории (принадлежащей А. Гротендику) можно найти в лекциях Хартшорна [1*] или в семинаре Гротендика [5*]. — *Прим. перев.*

2) $\Rightarrow$ 1). Функторы $X \to \varinjlim_{V,\,\mathrm{Cor}} \mathrm{Hom}_{\mathbf{Z}}(H^q(V, X), \mathbf{Q}/\mathbf{Z})$ образуют ∂-функтор. Поскольку G-модуль $\mathbf{Z}/p^m\mathbf{Z}$ обладает композиционным рядом, факторы которого изоморфны $\mathbf{Z}/p\mathbf{Z}$, то для любого целого m

$$\varinjlim_{V,\,\mathrm{Cor}} \mathrm{Hom}_{\mathbf{Z}}(H^q(V, \mathbf{Z}/p^m\mathbf{Z}), \mathbf{Q}/\mathbf{Z}) = \{0\}, \quad q \neq n,$$

откуда, используя предложение 3.1 (5), получаем, что G — группа Коэна — Маколея. Остается показать, что дуализирующий модуль $\hat{I}^p$ делим. Однако, применяя еще раз теорему двойственности и переходя к пределу по открытым подгруппам, получаем изоморфизм

$$\mathrm{Ext}^1_{\mathbf{Z}}(\mathbf{Z}/p\mathbf{Z}, I^p) \to \varinjlim_{V,\,\mathrm{Cor}} \mathrm{Hom}_{\mathbf{Z}}(H^{n-1}(V), \mathbf{Q}/\mathbf{Z}),$$

откуда следует нужный результат (предполагается, что $n > 0$, случай $n = 0$ тривиален).

Пусть G — группа Коэна — Маколея строго относительно p. Пусть X — конечный p-периодический G-модуль. Положим

$$\tilde{X} = \mathrm{Hom}_{\mathbf{Z}}(X, \hat{I}^p).$$

Тогда $\tilde{X}$ является дискретным p-периодическим G-модулем. Функтор $X \to \tilde{X}$ точен (модуль $\hat{I}^p$ делим).

4.4. Предложение. *Изоморфизм двойственности определяет изоморфизм ∂-функторов*

$$\mathrm{Hom}_{\mathbf{Z}}(H^q(G, X), \mathbf{Q}/\mathbf{Z}) \rightleftarrows H^{n-q}(G, \tilde{X}).$$

Этот изоморфизм индуцирован $\cup$-произведением

$$H^q(G, X) \times H^{n-q}(G, \tilde{X}) \xrightarrow{\cup} H^n(G, \hat{I}^p)$$

и каноническим гомоморфизмом

$$\rho \colon H^n(G, \hat{I}^p) \to \mathbf{Q}/\mathbf{Z}.$$

Доказательство. Действительно, теорема двойственности записывается в виде

$$\mathrm{Hom}_{\mathbf{Z}}(H^q(G, X), \mathbf{Q}/\mathbf{Z}) \rightleftarrows \mathrm{Ext}^{n-q}_G(X, \hat{I}^p).$$

Но X — модуль конечного типа, а $\hat{I}^p$ делим. Следствие 2.5 дает в этом случае изоморфизм

$$\operatorname{Ext}_G^{n-q}(X, \hat{I}^p) \xrightarrow{\sim} H^{n-q}(G, \operatorname{Hom}_{\mathbf{Z}}(X, \hat{I}^p)) = H^{n-q}(G, \tilde{X}),$$

откуда получаем искомый изоморфизм. Вторая часть предложения вытекает из того, что изоморфизм двойственности индуцирован $\cup$-произведением.

4.5. Определение. Проконечная группа G называется *группой Пуанкаре относительно p*, если она является группой Коэна — Маколея в строгом смысле относительно p, а ее дуализирующий модуль изоморфен как абелева группа группе $\mathbf{Q}_p/\mathbf{Z}_p$.

4.6. Предложение. *Пусть G — про-p-группа, для которой $\operatorname{cd}_p(G) = n$. Следующие свойства эквивалентны:*

1) *G — группа Пуанкаре относительно p;*

2) *$H^q(G)$ являются конечномерными векторными пространствами; $H^n(G)$ одномерно; $\cup$-произведение*

$$H^q(G) \times H^{n-q}(G) \xrightarrow{\cup} H^n(G)$$

определяет невырожденную билинейную форму.

1) $\Rightarrow$ 2) Заметим прежде всего, что G-подмодуль модуля $\hat{I}^p$, являющийся ядром умножения на p, изоморфен как абелева группа группе $\mathbf{Z}/p\mathbf{Z}$; группа G действует на нем тривиально (G — про-p-группа). Изоморфизм двойственности $\operatorname{Hom}_{\mathbf{Z}}(H^n(G), \mathbf{Q}/\mathbf{Z}) \xrightarrow{\sim} \operatorname{Hom}_G(\mathbf{Z}/p\mathbf{Z}, \hat{I}^p) \xrightarrow{\sim} \mathbf{Z}/p\mathbf{Z}$ показывает, что $H^n(G)$ одномерно. Далее, поскольку G-модуль $\mathbf{Z}/p\mathbf{Z}$ изоморфен G-модулю $\mathbf{Z}/p\mathbf{Z}$, предложение 4.4 дает изоморфизм $\operatorname{Hom}_{\mathbf{Z}}(H^q(G), \mathbf{Z}/p\mathbf{Z}) \to H^{n-q}(G)$, который показывает, что векторные пространства $H^q(G)$ изоморфны своим бидвойственным пространствам, а следовательно, что они конечномерны. Кроме того, с помощью предложения 4.4 легко проверяется, что предыдущий изоморфизм индуцирован $\cup$-произведением

$$H^q(G) \times H^{n-q}(G) \xrightarrow{\cup} H^n(G),$$

откуда вытекает, что $\cup$-произведение невырождено.

2) $\Rightarrow$ 1) Эта импликация уже была доказана (гл. I, § 4, п. 5, доказательство предложения 30).

4.7. Предложение. *Пусть G — проконечная группа конечной когомологической p-размерности. Предположим, что существует открытая подгруппа V группы G, являющаяся группой Коэна — Маколея относительно p (соответственно группой Коэна — Маколея в строгом смысле относительно p или группой Пуанкаре относительно p). Тогда группа G является группой того же типа. Справедливо и обратное, т. е. если G — группа Коэна — Маколея относительно p (соответственно группа Коэна — Маколея в строгом смысле относительно p или группа Пуанкаре относительно p), то каждая открытая подгруппа V группы G является группой того же типа.*

Этот результат тривиально следует из определения и предложения 3.8.

Лазар доказал, что если G — аналитическая группа над $\mathbf{Q}_p$ размерности n, то каждая ее достаточно малая открытая подгруппа является группой Пуанкаре.

4.8. Следствие. *Пусть G — аналитическая группа над полем $\mathbf{Q}_p$ размерности n. Предположим, что она компактна и имеет конечную когомологическую p-размерность. Тогда G — группа Пуанкаре относительно p.*

Упражнения. 1) G — проконечная группа, порядок которой делится на p^∞. Показать, что $H^0(\tilde{I}_G^p) = \{0\}$.

2) Пусть G — группа Коэна — Маколея относительно p и $n = \mathrm{cd}_p(G)$. Доказать эквивалентность следующих утверждений.

„G — группа Коэна — Маколея в строгом смысле относительно p“ $\Leftrightarrow \varinjlim_{V,\, \mathrm{Cor}} \mathrm{Hom}_{\mathbf{Z}}(H^{n-1}(V), \mathbf{Q}/\mathbf{Z}) = \{0\}$.

3) Пусть p-размерность группы G равна 1. Показать, что G является группой Коэна — Маколея в строгом смысле относительно p.

4) Пусть $F(J)$ — свободная p-группа, $\{\sigma_i\}_{i \in J}$ — ее образующие, (σ_i) — замкнутые подгруппы, порожденные образующими. Показать, что дуализирующий модуль $F(J)$ равен $\prod_{i \in J} M_G^{(\sigma_i)}(\mathbf{Q}_p/\mathbf{Z}_p)$.

ЛИТЕРАТУРА

Альберт, Джекобсон (Albert A., Jacobson N.).
[1] On reduced exceptional simple Jordan algebras, *Ann. Math.*, **66** (1957), 400—417.

Акс (Ax J.).
[1] Proof of some conjectures on cohomological dimension, *Proc. Amer. Math. Soc.*, **16** (1965), 1214—1221.

Артин (Artin E.).
[1*] The theory of braids, *Amer. Scientist*, **38** (1950), 111—119.

Артин, Тейт (Artin E., Tate J.).
[1] Class field theory, Harvard, 1961.

Бальдассари (Baldassarry M.).
[1*] Алгебраические многообразия, ИЛ, М., 1961.

Борель (Borel A.).
[1] Groupes linéaires algébriques, *Ann. Math.*, **64** (1956), 20—82.
[2] Some finiteness properties of adele groups over number fields, Publ. Math. IHES, 1963, № 16.
[3] Arithmetic properties of linear algebraic groups, Proc. Cong. Stockholm, 1962, 10—22.

Борель, Хариш-Чандра (Borel A., Harish-Chandra).
[1] Arithmetic subgroups of algebraic groups, *Ann. Math.*, **75** (1962), 485—535. (Русский перевод: Борель А., Хариш-Чандра, Арифметические подгруппы алгебраических групп, сб. *Математика*, **8**:2 (1964), 19—73.)

Борель, Серр (Borel A., Serre J. P.).
[1] Théorèmes de finitude en cohomologie galoisienne, *Comm. Math. Helv.*, **39** (1964), 111—164.

Боревич З. И., Шафаревич И. Р.
[1*] Теория чисел, «Наука», М., 1964.

Бурбаки (Bourbaki N.).
[1] Topologie generale, 3^{me} edition, Paris, Hermann.
[2] Groupes et algebres de Lie, Chap. I. Algebres de Lie, Paris, Hermann.
[3*] Алгебра. Многочлены и поля. Упорядоченные группы, «Наука», М., 1965.
[4*] Алгебра. Модули, кольца, формы, «Наука», М., 1966.

---

[1]) Звездочкой отмечена литература, добавленная при переводе. — *Прим. ред.*

Ван дер Варден (Waerden B. L. van der).
[1*] Современная алгебра, т. 1, 2, Гостехиздат, М., 1947.

Вейль (Weil A.).
[1] On algebraic groups and homogeneous spaces, *Amer. J. Math.*, **77** (1955), 493—512.
[2] The field of definition of a variety, *Amer. J. Math.*, **78** (1956), 509—524.
[3] Algebras with involutions and the classical groups, *Journ. Ind. Math. Soc.*, **24** (1960), 589—623.
[4] Adeles and algebraic groups (notes by M. Demazure and T. Ono), Inst. Adv. Studies, Princeton, 1961. (Русский перевод: Вейль А., Адели и алгебраические группы, сб. *Математика*, **8** : 4 (1964), 3—74.)

Витт (Witt E.).
[1] Theorie der quadratischen Formen in beliebigen Körpern, *Journal für Reine und Angew. Mat.*, **176** (1937), 31—44.

Габриэль (Gabriel P.).
[1] Des catégories abéliennes, *Bull. Soc. Math. France*, **90** (1962), 323—448.

Гертциг (Hertzig D.).
[1] Forms of algebraic groups, *Proc. Amer. Math. Soc.*, **12** (1961), 657—660.

Годеман (Godement R.).
[1] Groupes lineaires algébriques sur un corps parfait, Séminaire Bourbaki, 1960—1961, exposé 206.
[2] Domaines fondamentaux des groupes arithmetiques, Séminaire Bourbaki, 1962—1963, exposé 257.

Голод Е. С., Шафаревич И. Р.
[1] О башне полей классов, *Изв. АН СССР, сер. мат.*, **28** (1964), 261—272.

Гротендик (Grothendieck A.).
[1] Sur quelques points d'algebre homologique, *Tôhoku Math. J.*, **9** (1957), 119—221. (Русский перевод: Гротендик А., О некоторых вопросах гомологической алгебры, ИЛ, М., 1961.)
[2] A general theory of fibre spaces with structure sheaf, Univ. Kansas, Report № 4, 1955.
[3] Technique de descente et théorèmes d'existence en géométrie algébrique, II: le théorème d'existence en theorie formelle des modules, Seminaire Bourbaki, 1959—1960, exposé 195.
[4] Eléments de géométrie algébrique (rédigé en collaboration avec J. Dieudonné), Publ. Math. IHES, 1960—. . ., № 4, 8, 11, 17, 20, 24, 28, 32, ...
[5*] Cohomologie locale des faisceaux coherents et theorems de Lefschets locaux et globaux, Seminaire de Geometrie algebrique IHES, 1962.

Дедекер (Dedecker P.).
[1] Sur la cohomologie non abelienne, I, *Canad. J. Math.*, **12** (1960), 231—251; II, ibid., **15** (1963), 84—93.

Дельзант (Delzant A.).
[1] Definitions des classes de Stiefel-Whitney d'un module quadratique sur un corps de caracteristique differente de 2, *C. R. Acad. Sci.*, **255** (1962), 1366—1368.

Демазур, Гротендик (Demazure M. et Grothendieck A.).
[1] Schemas en groupes, Séminaire de Geométrie Algébrique IHES, 1962—1964.

Дёмушкин С. П.
[1] Группа Галуа максимального *p*-расширения локального поля, *ДАН СССР*, **128** (1959), 657—660.
[2*] Топологические 2-группы с четным числом образующих и одним полным определяющим соотношением, *Изв. АН СССР*, сер. мат., **29** (1965), 3—10.

Джекобсон (Jasobson N.).
[1] Composition algebras and their automorphisms, *Rend. Circolo Mat. Palermo*, **7** (1958), 1—26.

Джорджутти (Giorgiutti I.).
[1] Groupes de Grothendieck, a paraitre dans les *Ann. Fac. Sci. de Toulouse*.

Дьедонне (Dieudonné J.).
[1] La geometrie des groupes classiques, *Ergebn. angew. Math.*, Heft 5, 1955.
[2*] Алгебраическая геометрия, сб. *Математика,* **9** : **1** (1965), 54—126.

Дуади (Douady A.).
[1] Cohomologie des groups compacts totalment discontinus, Seminaire Bourbaki, 1959—1960, expose 189.

Ивасава (Iwasawa K.).
[1] On solvable extensions of algebraic number fields. *Ann. Math.*, **58** (1953), 548—572.
[2] On Galois groups of local fields, *Trans. Amer. Math. Soc.*, **80** (1955), 448—469.
[3] A note on the group of units of an algebraic number field, *J. Math. pures et appl.*, **35** (1956), 189—192.

Картан, Эйленберг (Cartan A., Eelenberg S).
[1] Homological algebra, Princeton Math. Ser., № 19, Princeton, 1956. (Цитируется как [M].) (Русский перевод: Картан А., Эйленберг С., Гомологическая алгебра, ИЛ, М., 1960).

Картье (Cartier P.).
[1] Groupes algebriques et groupes formels, Colloque de Bruxelles, 1962, 87—111.

Касселс (Cassels J.).
[1] Arithmetic on an elliptic curve, Proc. Cong. Stockholm, 1962, 234—246.

Кавада (Kawada Y.).
[1] On the structure of the Galois group of some infinite extensions, I, *J. Fac. Sci. Tokyo*, **7** (1954), 1—18; II, ibid., 87—106.
[2] Cohomology of group extensions, *Journ. Fac. Sci. Tokyo*, **9** (1963), 417—431.

Кнезер (Kneser M.).
[1] Schwache Approximation in algebraischen Gruppen, Colloque de Bruxelles, 1962, 41—52.
[2] Einfach zusammenhängende algebraische Gruppen in der Arithmetik, Proc. Cong. Stockholm, 1962, 260—263.
[3] Galois-Kohomologie halbeinfacher algebraischer Gruppen über p-adischen Körpern, I, *Math. Z.*, **88** (1965), 40—47; II, ibid., **89** (1965), 250—273.

Костант (Kostant B.).
[1] The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group, *Amer. J. Math*, **81** (1959), 973—1032.

Краснер (Krasner M.).
[1] Nombre des extensions d'un degré donné d'un corps p-adique (cinq notes), *C. R. Acad. Sci.*, **254** (1962), 3470—3472; ibid. 255.
[2*] Nombre des extensions d'un degré donné d'un corps p-adique, Les tendances geometriques en algebre et theorie des nombres, Colloq. Internat. du Centre National de la Recherche Scientif., Clermont—Ferrand (2—9 Avril 1964), Paris, CNRS, 1966.

Кроуэлл Р., Фокс Р (Crowell R., Fox R.).
[1] Введение в теорию узлов, «Мир», М., 1967.

Лабют (Labute J.).
[1*] Classification des groupes de Demuškin, *C. R. Acad. Sci.*, **260** (1965), 1043—1047.

Лазар (Lazard M.).
[1] Sur les groupes nilpotents et les anneaux de Lie, Annales ENS, 71 (1954), 101—190. (Цитируется как [L].)
[2] Groupes analytiques p-adiques. Publ. Math. IHES, № 26 (1965).

Ленг (Lang S.).
[1] On quasi-algebraic closure, *Ann. Math.*, **55** (1952), 373—390.
[2] Algebraic groupes over finite fields. *Amer. Journ. Math.*, **78** (1956), 555—563.
[3] Some theorems and conjectures in diophantine equations, *Bull Amer. Math. Soc.*, **66** (1960), 240—249.
[4*] Алгебраические числа, «Мир», М., 1966.

Ленг, Тейт (Lang S., Tate J.).
[1] Principles homogeneous spaces over abelian varieties, *Amer. Journ. of Maths.*, **78** (1956), 659—684.

Маклейн (Maclane S.).
[1*] Гомология, «Мир», М., 1966.

Мамфорд (Mumford D.).
[1*] Lectures on algebraic curves on an algebraic surfaces, Ann. Math. Studies, № 59, Princeton Univ. Press, 1966. (Готовится русский перевод в изд-ве «Мир».)

Манин Ю. И.
[1*] Алгебраическая топология алгебраических многообразий, *УМН*, **20** (1965), вып. 6, 1—12.

Менникe (Mennicke J.).
[1] Einige endliche Gruppen mit drei Erzengenden und drei Relationen, *Arch. Math.*, **10** (1959), 409—418.

Нагата (Nagata M.).
[1] Note on a paper of Lang concerning quasi-algebraic closure, *Mem. Univ. Kyoto*, **30** (1957), 237—241.

Оно (Ono T.).
[1] Arithmetic of algebraic tori. *Ann. Math.*, **74** (1961), 101—139.
[2] On the Tamagawa number of algebraic tori, *Ann. Math.*, **78** (1963), 47—73.
[3] On the relative theory of Tamagawa numbers. *Ann. Math.* **82** (1965), 88—111.

Пуату (Poitou G.).
[1] Seminaire de Lille, 1962—1963.

Розенлихт (Rosenlicht M.).
[1] Some basic theorems on algebraic groups, *Amer. J. Math.*, **78** (1956), 401—443.
[2] Some rationality questions on algebraic groups., *Ann. Mat. Pura et Apll.*, **43** (1957), 25—50.

Серр (Serre J. P.)
[1] Corps locaux, Act. Sci. Ind., № 1296, Paris, 1962. (Цитируется как [CL].)
[2] Cohomologie galoisienne des groupes algébriques linéaires, Colloque de Bruxelles, 1962, 53—67.
[3] Structure de certains pro-p-groupes (d'apres Demuškin), Seminaire Bourbaki, 1962—1963, expose 252.
[4] Sur les groupes de congruence des variétés abéliennes, *Изв. АН СССР*, сер. матем., **28** (1964), 3—20.
[5] Sur la dimension cohomologique des groupes profinis, *Topology*, **3** (1965), 413—420.
[6*] Groupes algebrique et corps de classes, Paris, Hermann, 1959. (Готовится русский перевод в изд-ве «Мир».)
[7*] Локальная алгебра и теория кратностей, сб. *Математика*, **7**:5 (1963), 3—93.

Спрингер (Springer T.).
[1] On the equivalence of quadratic forms, Proc. Acad. Amsterdam, **62** (1959), 241—253.
[2] The classification of reduced exceptional simple Jordan algebras, *Proc. Acad. Amsterdam*, **63** (1960), 414—422.
[3] Quelques resultats sur la cohomologie galoisienne, Colloque de Bruxelles, 1962, 129—135.

С у о н (S w a n R.).
[1] Induced representations and projective modules. Ann. of Maths., **71** (1960), 552—578. (Русский перевод: С у о н Р., Индуцированные представления и проективные модули, сб. *Математика*, 8 : 1 (1964), 3—29.)
[2] The Grothendieck ring of a finite group, *Topology*, **2** (1963), 85—110.

Т е й т (T a t e J.).
[1] *WC*-groups over *p*-adic fields, Seminaire Bourbaki, 1957—1958, expose 156.
[2] Galois cohomology of abelian varieties over *p*-adic fields, Notes polycopiées rédigées par S. Lang, 1959.
[3] Duality theorems in Galois cohomology over number fields, Proc. Cong. Stockholm, 1962, 288—295.

Т и т ц (T i t s J.).
[1] Groupes simples et geometries associees, Proc. Cong. Stockholm, 1962, 197—221.
[2] Groupes semi-simples isotropes, Colloque de Bruxelles, 1962, 137—147.

Х а р т ш о р н (H a r t s h o r n R.).
[1*] Residues and duality, Lecture notes, № 20, Springer, 1966.

Х о л л (H a l l M.).
[1] Теория групп, ИЛ, М., 1962.

Х о х ш и л ь д (H o c h s c h i l d G.).
[1] Simple algebras with purely inseparable splitting fields of exponent 1, *Trans. Amer. Math. Soc.*, **79** (1955), 477—489.
[2] Restricted Lie algebras and simple associative algebras of characteristic *p*, *Trans. Amer. Math. Soc.*, **80** (1955), 135—147.

Х о х ш и л ь д, С е р р (H o c h s c h i l d G., S e r r e J. P.).
[1] Cohomology of group extensions, *Trans. Amer. Math. Soc.*, **74** (1953).

Ц а с с е н х а у з (Z a s s e n h a u s H.).
[1] The theory of groups, N. Y., 1958.

Ч о у (C h o w W.).
[1*] On the projective embedding of homogenious varieties, Symposium in honour of S. Lefschetz, Princeton, 1957, 122—128

Ш а т а л ь е (C h â t e l e t F.).
[1] Variations sur un theme de H. Poincare, Annales ENS, **61** (1944), 249—300.
[2] Methodes galoisiennes et courbes de genre 1, *Ann, Univ. Lyon*, Sect. A-IX (1946), 40—49.

Ш а т ц (S h a t z S.).
[1] Cohomology of artinian group schemes over local fields, *Ann. Math.*, **79** (1964), 411—449.

Ш а ф а р е в и ч И. Р.
[1] О *p*-расширениях, *Мат. сб.*, **20** (1947), 351—363.
[2] О бирациональной эквивалентности эллиптических кривых, *ДАН СССР*, **114** (1957), 267—270.

[3] Поля алгебраических чисел, Proc. Cong. Stockholm, 1962.
[4] Расширения с заданными точками ветвления, Publ. Math. IHES, 18 (1964), 295—316.

Шевалле (Chevalley C.).
[1] Sur certain groupes simples, *Tohoku Math. J.*, **7** (1955), 14—66.
[2] Classification des groupes de Lie algebriques, Seminaire ENS, 1956—1958.
[3] Certain schemes de groupes semi-simples, Seminaire Bourbaki, 1960—1961, expose 219.
[4] Theorie des groupes de Lie, Paris, Hermann, 1951. (Русский перевод: Шевалле К., Теория групп Ли, ИЛ, М., 1958.)
[5*] Введение в теорию алгебраических функций от одного переменного, Физматгиз, М., 1959.

Штейнберг (Steinberg R.).
[1] Regular elements of semisimple algebraic groups, Publ. Math. IHES, 25 (1965), 281—312.

ОГЛАВЛЕНИЕ

Ж.-П. Серр

КОГОМОЛОГИИ ГАЛУА

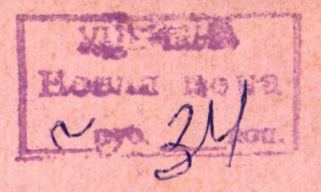
Редактор *Г. М. Цукерман*
Художник *С. Т. Еременко.* Художественный редактор *В. И. Шаповалов*
Технический редактор *Н. А. Иовлева*

Сдано в производство 12/IV-1968 г. Подписано к печати 11/IX-1968 г.
Бумага № 3 $84\times108^1/_{32}$=3,25 бум. л., 10,92 усл. печ. л.
Уч.-изд. л. 9,78. Изд. № 1/4466. Цена 67 к. Зак. 1202.
(Темплан 1968 г. изд-ва „Мир“, пор. № 31)

ИЗДАТЕЛЬСТВО „МИР“, Москва, 1-й Рижский пер., 2

Ленинградская типография № 2 имени Евгении Соколовой
Главполиграфпрома Комитета по печати при Совете Министров СССР
Измайловский проспект, 29

67 коп.






Ж.-П. СЕРР
Когомологии Галуа